




Post-Graduate Diploma in Cyber Security
Practical Handbook of Internet Security for
Beginners
(PGDCS-04)

Title	Practical Handbook of Internet Security for Beginners
Advisors	Mr. R. Thyagarajan , Head, Admn. & Finance and Acting Director, CEMCA Dr. Manas Ranjan Panigrahi , Program Officer (Education), CEMCA Prof. Durgesh Pant , Director- SCS&IT, UOU
Editor	Er. Ashutosh Bahuguna , Scientist-C, Cert-In, Ministry of Communication & IT, Govt. of India
Author	Dr. Jeetendra Pande , Assistant Professor- School of CS & IT, Uttarakhand Open University, Haldwani
ISBN: 978-93-84813-91-8	
Acknowledgement	
The University acknowledges with thanks the expertise and financial support provided by Commonwealth Educational Media Centre for Asia (CEMCA), New Delhi, for the preparation of this study material.	
 Uttarakhand Open University, 2016 © Uttarakhand Open University, 2016. Practical Handbook of Internet Security for Beginners is made available under a Creative Commons Attribution Share-Alike 4.0 License (international): http://creativecommons.org/licenses/by-sa/4.0/ It is attributed to the sources marked in the References, Article Sources and Contributors section.	
Published by: Uttarakhand Open University, Haldwani March, 2016	

Expert Panel	
S. No.	Name
1	Dr. Jeetendra Pande, School of Computer Science & IT, Uttarakhand Open University, Haldwani
2	Prof. Ashok Panjwani, Professor, MDI, Gurgaon
3	Group Captain Ashok Katariya, Ministry of Defense, New Delhi
4	Mr. Ashutosh Bahuguna, Scientist-CERT-In, Department of Electronics & Information Technology, Government of India
5	Mr. Sani Abhilash, Scientist-CERT-In, Department of Electronics & Information Technology, Government of India
6	Wing Commander C.S. Chawla, Ministry of Defense, New Delhi
7	Mr. Mukesh Kumar Verma, IT Consultant, Chandigarh
8	Mr. Pritam Dutt Gautam, IT Consultant, New Delhi

INDEX

1.1 LEARNING OBJECTIVES	1
1.2 HOW TO GENERATE SECURE PASSWORD.....	1
1.2.1 Guideline for setting secure Password	1
1.2.2 Guidelines for using Password Manager	5
1.2.2.1 KeePassX	6
1.2.2.2 Clipperz	7
1.2.2.3 Password Gorilla	8
1.2.2.4 Gpassword Manager	9
1.2.2.5 Password Safe	10
1.2.3 Guidelines for Two-step Verification.....	11
1.3 CONFIGURING FIREWALL IN YOUR COMPUTER	22
1.3.1 How to Configure Your Mac's Firewall	22
1.3.1.1 Turning on and Configuring the Mac OS X Firewall	22
1.3.2 Working with Windows Firewall in Windows 7	25
1.3.2.1 Firewall in Windows 7	25
1.3.2.2 Configuring Windows Firewall	26
1.3.3 How to Start & Use The Windows Firewall with Advanced Security.....	30
1.3.3.1 How to Access the Windows Firewall with Advanced Security	30
1.3.3.2 What Are The Inbound & Outbound Rules?	32
1.3.3.3 What Are The Connection Security Rules?	34
1.3.3.4 What Does the Windows Firewall with Advanced Security Monitor?.....	35
1.4 STEPS TO FIND THE BEST BROWSER ACCORDING TO THE USERS REQUIREMENT	37
1.5 SAFE BROWSING	43
1.5.1 How do I know if a website is secure?	43
1.5.2 Tips for buying online	43
1.6 CLEARING CACHE FOR BROWSERS	46
1.6.1 Clearing cache for Chrome Browsers above version 10	46
1.6.2 Clearing cache for Chrome Browsers from version 1 to 9	49
1.6.3 Clearing cache for Safari for iOS, iPhone and iPad	51
1.6.4 Clearing cache for Safari for Mac os x	53
1.6.5 Clearing cache for Safari for windows.....	54
1.6.6 Clearing cache for Internet explorer 9, 10 and 11	55

1.6.7 Clearing cache for Internet explorer 8	58
1.6.8 Clearing cache for Firefox.....	60
1.6.9 Clearing cache for firefox 33	62
1.6.10 Clearing cache for opera.....	64
1.6.11 Clearing cache for Ccleaner	65
1.7 WIRELESS SECURITY – BEST PRACTICES.....	67
1.7.1 What is Wireless LAN?.....	67
1.7.2 Major issues with WLAN	68
1.8 PROTECT YOURSELF AND YOUR DATA WHEN USING SOCIAL NETWORKING SITES	73
1.8.1 General Tips on using Social Networking platforms safely	74
1.8.2 Posting Personal Details	75
1.8.3 Friends, Followers and Contacts	75
1.8.4 Status Updates	76
1.8.5 Sharing Online Content.....	76
1.8.6 Revealing your Location	77
1.8.7 Sharing Videos and Photos	77
1.8.8 Instant Chats	77
1.8.9 Joining and Creating Groups, Events and Communities.....	77
1.9 EMAIL SECURITY TIPS.....	79
1.10 SMARTPHONE SECURITY GUIDE	81
1.10.1 Introduction to Smartphone Security	82
1.10.1.1 Purses, Wallets, Smartphones	82
1.10.2 Platforms, Setup and Installation.....	83
1.10.2.1 Platforms and Operating Systems	83
1.10.2.2 Feature Phones	84
1.10.2.3 Branded and locked smartphones	84
1.10.2.4 General Setup	84
1.10.2.5 Installing and updating applications	84
1.10.3 Communicating Securely(Through Voice and Messages) with a Smartphone	85
1.10.3.1 Secure Voice Communication	85
1.10.3.2 Sending Messages Securely	88
1.10.3.3 Storing Information on your Smartphone	89
1.10.3.4 Sending Email from your Smartphone	90
1.10.3.5 Capturing Media with your Smartphone	91

1.10.3.6 Accessing the Internet Securely from your Smartphone.....	91
1.10.3.7 Advanced Smart Phone Security.....	92
1.11 SECURING COMPUTER USING FREE ANTIVIRUS.....	95
1.12 PROTECTING THE SENSITIVE FILES ON YOUR COMPUTER.....	98
1.12.1 Introduction to Secure File Storage.....	98
1.12.1.1 Encrypting your Information.....	98
1.12.1.2 Tips on using File Encryption Safely.....	98
1.12.2. Hiding your Sensitive Information	100
1.12.2.1 Considering the risk of Self-Incrimination	100
1.12.2.2. Considering the risk of Identifying your sensitive Information	101
1.13 WHAT IS A SOFTWARE PATCH?.....	103
1.13.1 Creating a Patch	103
1.13.2 Applying a Patch.....	104
1.13.3 Is It Really That Simple?	105
1.13.3.1 Release Early, Release Often.....	106
1.13.3.4 Why Should I Contribute A Patch?	106
References, Article Source & Contributors	107

UNIT I: Generating Secure Passwords

1.1 LEARNING OBJECTIVES

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
- Configure firewall on Mac, Windows and Linux based system
- Evaluate and select best browser based on your need
- Perform safe browsing
- Use different cache clearing techniques
- Understand and apply the best wireless security practices
- Protect yourself and your data while using social networking sites
- Use email securely
- Handle your Smartphone securely
- Evaluate and use various free antivirus available over internet
- Protect your sensitive files on your computer
- Apply and update software patch in your system

1.2 HOW TO GENERATE SECURE PASSWORD

1.2.1 Guideline for setting secure Password¹

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"

¹ http://www.lockdown.co.uk/?pg=password_guide

- ✓ 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 users name, also too short.
- ✓ "christine" - The name of the users girlfriend, easy to guess
- ✓ "kciredref" - The users name backwards
- ✓ "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 else's.

- ✓ "mItWdOtW4Me" - **Monday is the worst day of the week for me.**

How would a potential hacker get hold of my password anyway?

There are four main techniques hackers can use to get hold of your password:

1. **Steal it.** That means looking over your shoulder when you type it, or finding the paper where you wrote it down. This is probably the most common way passwords are compromised, thus it's very important that if you do write your password down you keep the paper extremely safe. Also remember not to type in your password when somebody could be watching.
2. **Guess it.** It's amazing how many people use a password based on information that can easily be guessed. Psychologists say that most men use 4 letter obscenities as passwords and most women use the names of their boyfriends, husbands or children.
3. **A brute force attack.** This is where every possible combination of letters, numbers and symbols in an attempt to guess the password. While this is an extremely labour intensive task, with modern fast processors and software tools this method is not to be underestimated. A Pentium 100 PC might typically be able to try 200,000 combinations every second this would mean that a 6 character password containing just upper and lower case characters could be guessed in only 27½ hours.
4. **A dictionary attack.** A more intelligent method than the brute force attack described above is the dictionary attack. This is where the combinations tried are first chosen from words available in a dictionary. Software tools are readily available that can try

every word in a dictionary or word list or both until your password is found. Dictionaries with hundreds of thousands of words, as well as specialist, technical and foreign language dictionaries are available, as are lists of thousands of words that are often used as passwords such as "qwerty", "abcdef" etc.

1.2.2 Guidelines for using Password Manager²

We use passwords to ensure security and the confidentiality of our data. One of the biggest modern day crimes is identity theft, which is easily accomplished when passwords are compromised. The need of the hour is good password management.

Password Manager

Have you ever thought of an alternative to remembering your passwords and not repeatedly entering your login credentials? Password managers are one of the best ways to store, back up and manage your passwords. A good password is hard to remember and that's where a password manager comes in handy. It encrypts all the different passwords that are saved with a master password, the only one you have to remember.

What is a password manager?

A password manager is software that helps a user to manage passwords and important information so that it can be accessed any time and anywhere. An excellent password manager helps to store information securely without compromising safety. All the passwords are saved using some kind of encryption so that they become difficult for others to exploit.

Why you should use it?

If you find it hard to remember passwords for every website and don't want to go through the 'Forgot password?' routine off and on, then a password manager is what you are looking for. These are designed to store all kinds of critical login information related to different websites.

How does it work?

Password managers may be stored online or locally. Online password managers store information in an online cloud, which can be accessed any time from anywhere. Local password managers store information on the local server, which makes them less accessible. Both have their own advantages, and the manager you use would depend on your need.

Online password managers use browser extensions that keep data in a local profile, syncing with a cloud server. Some other password managers use removable media to save the password so that you can carry it with you and don't have to worry about online issues. Both

² <http://opensourceforu.ifytimes.com/2015/01/peek-top-password-managers/>

these options can also be combined and used as two-factor authentication so that data is even more secure.

The passwords are saved using different encryptions based on the services that the companies provide. The best password managers use a 256-bit (or more) encryption protocol for better security, which has been accepted by the US National Security Agency for top secret information handling. If you have considered using a password manager and haven't decided on one, this section features the top five.

1.2.2.1 KeePassX

KeePassX is an open source, cross-platform and light weight password management application published under the terms of the GNU General Public License. It was built based on the Qt Libraries. KeePassX stores information about user names, passwords and other login information in a secure database.

KeePassX uses its own random password generator, which makes it easier to create strong passwords for better security. It also includes a powerful and quick search tool with which a keyword of a website can be used to find login credentials that have been stored in the database. It allows users to customise groups, making it more user friendly. KeePassX is not limited to storing only usernames and passwords but also free-form notes and any kind of confidential text files.

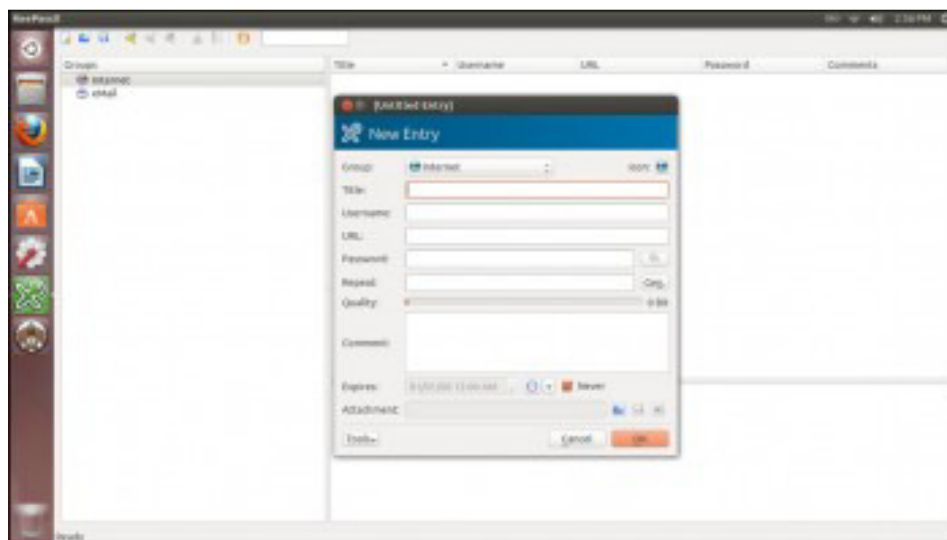


Figure 1: KeePassX

Features

- *Simple user interface*: The left pane tree structure makes it easy to distinguish between different groups and entries, while the right pane shows more detailed information.
- *Portable media access*: Its portability makes it easy to use since there's no need to install it on every computer.
- *Search function*: Searches in the complete database or in every group.
- *Auto fill*: There's no need to type in the login credentials; the application does it whenever the Web page is loaded. This keeps it secure from key loggers.
- *Password generator*: This feature helps to generate strong passwords that make it difficult for dictionary attacks. It can be customised.
- *Two factor authentication*: It enables the user to either unlock the database by a master password or by a key from a removable drive.
- *Adds attachments*: Any type of confidential document can be added to the database as an attachment, which allows users to secure not just passwords.
- *Cross-platform support*: It works on all supported platforms. KeePassX is an open source application, so its source code can be compiled and used for any operating system.
- *Security*: The password database is encrypted with either the AES encryption or the Twofish algorithm, which uses 256-bit key encryption.
- *Expiration date*: The entries can be expired, based on a user defined date.
- *Import and export of entries*: *Entries*: from PwManager or Kwallet can be imported, and entries can be exported as text files.
- *Multi-language support*: It supports 15 languages.

1.2.2.2 Clipperz

Clipperz is a Web-based, open source password manager built to store login information securely. Data can be accessed from anywhere and from any device without any installation. Clipperz also includes an offline version when an Internet connection is not available.

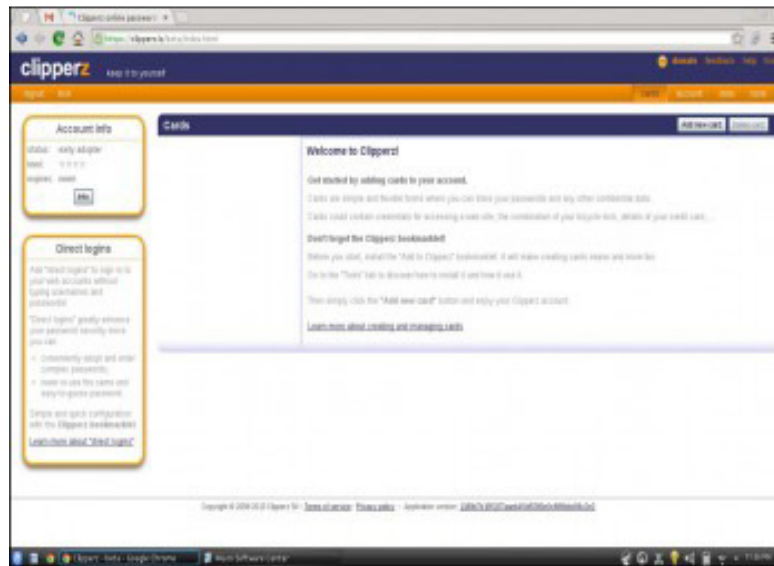


Figure 2: Clipperz

Features

- **Direct login:** Automatically logs in to any website without typing login credentials, with just one click.
- **Offline data:** With one click, an encrypted local copy of the data can be created as a HTML page.
- **No installation:** Since it's a Web-based application, it doesn't require any installation and can be accessed from any compatible browser.
- **Data import:** Login data can be imported from different supported password managers.
- **Security:** The database is encrypted using JavaScript code on the browser and then sent to the website. It requires a passphrase to decrypt the database without which data cannot be accessed.
- **Support:** Works on any operating system with a major browser that has JavaScript enabled.

1.2.2.3 Password Gorilla

Password Gorilla is an open source, cross-platform, simple password manager and personal vault that can store login information and notes. Password Gorilla is a Tcl/Tk application that runs on Linux, Windows and Mac OS X. Login information is stored in the database, which can be accessed only using a master password. The passwords are SHA256 protected and the database is encrypted using the Twofish algorithm. The key stretching feature makes it difficult for brute force attacks.

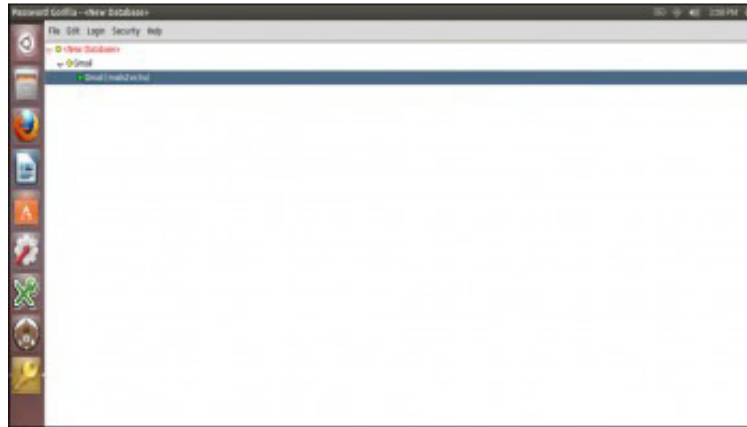


Figure 3: Password Gorilla

Features

- *Portable*: Designed to run on a compatible computer without being installed.
- *Import of database*: Can import the password database saved in the CSV format.
- *Locks the database when idle*: It automatically locks the database when the computer is idle for a specific period of time.
- *Security*: It uses the Twofish algorithm to encrypt the database.
- *Can copy credentials*: Keyboard shortcuts can be used to copy login credentials to the clipboard.
- *Auto clear*: This feature clears the clipboard after a specified time.
- *Organises groups*: Groups and sub-groups can be created to organise passwords for different websites.

1.2.2.4 Gpassword Manager

Gpassword Manager is a simple, lightweight and cross-platform utility for managing and accessing passwords. It is published under the terms of the Apache License. It allows users to securely store passwords/URLs in the database. The added entries can be marked as favourites, which then can be accessed by right-clicking the system tray icon. The passwords and other login information shown in the screen can be kept hidden based on user preferences.

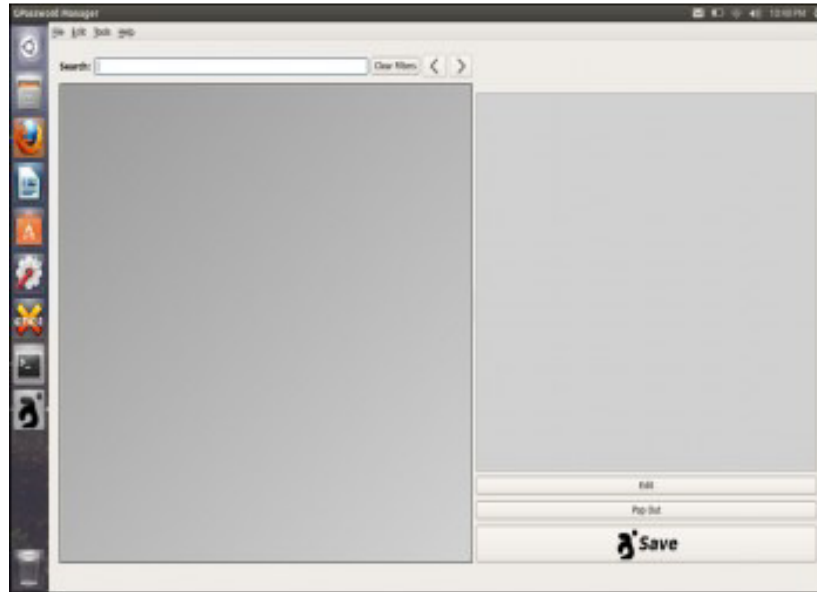


Figure 4: Gpassword manager

Features

- *Access to favourite sites:* A list of favourite Web pages can be accessed quickly from the convenient 'tray' icon.
- *Quick fill:* Passwords and other information can be clicked and dragged onto forms for quick filling out.
- *Search bar:* The quick search bar allows users to search passwords that are needed.
- *Password generator:* Passwords with user-defined options can be generated with just a click.
- *Quick launch:* Favourite websites can be launched by right-clicking the tray icon.

1.2.2.5 Password Safe

Password Safe is a simple and free open source application initiated by Bruce Schneier and released in 2002. Now Password Safe is hosted on SourceForge and developed by a group of volunteers. It's well known for its ease of use. It is possible to organise passwords based on user preference, which makes it easy for the user to remember. The whole database backup and a recovery option are available for ease of use. Passwords are kept hidden, making it difficult for shoulder surfing. Password Safe is licensed under the Artistic licence.



Figure 5: Password Safe

Features

- *Ease of use:* The GUI is very simple, enabling even a beginner to use it.
- *Multiple databases:* It supports multiple databases. And different databases can be created for each category.
- *Safe decryption:* The decryption of the password database is done in the RAM, which leaves no trace of the login details in the hard drive.
- *Password generator:* Supports the generation of strong, lengthy passwords.
- *Advanced search:* The advanced search function allows users to search within the different fields.
- *Security:* Uses the Twofish algorithm to encrypt the database.

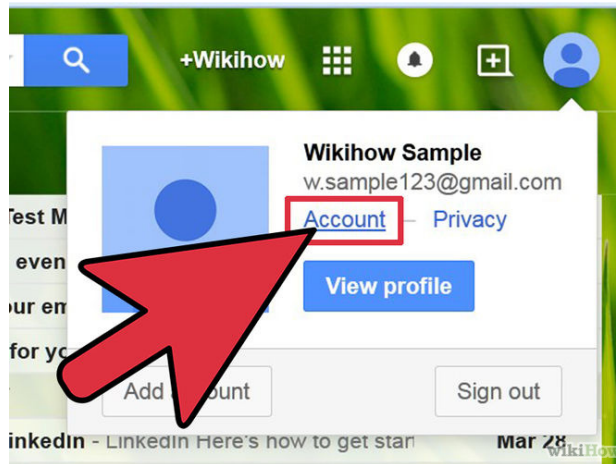
1.2.3 Guidelines for Two-step Verification³

Every day, tens of thousands of personal accounts are hacked. Personal information is compromised, passwords are cracked, and lives are put in jeopardy. If you ever use one password for multiple accounts, you are exponentially increasing your vulnerability to being hacked. Thankfully, Google has launched its **2-step verification system**: anytime an unknown device is used to sign into your Google account, the user has to provide a verification code *in addition* to the password. So it's not enough for hackers to just get your

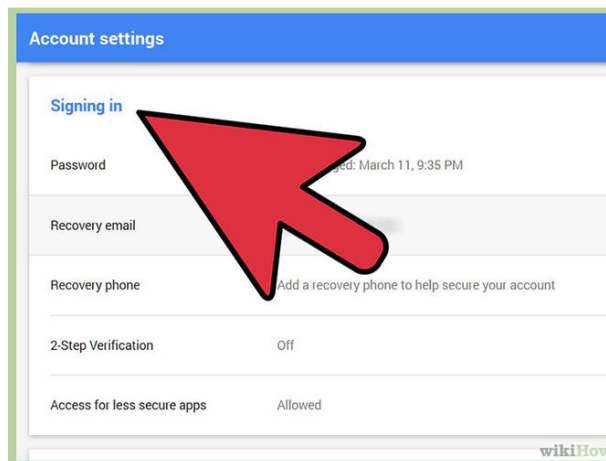
³ <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail>

password; they'll also need physical control of your phone or computer to access your account.

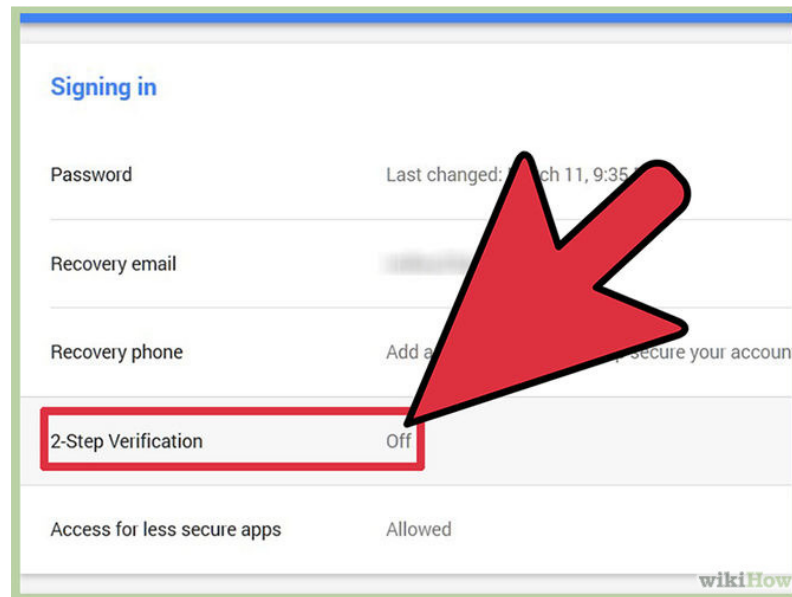
Step 1: Sign into your Gmail account. Click on a thumbnail of your avatar on the right side of the top menu bar, and then click "Account" to update your settings.



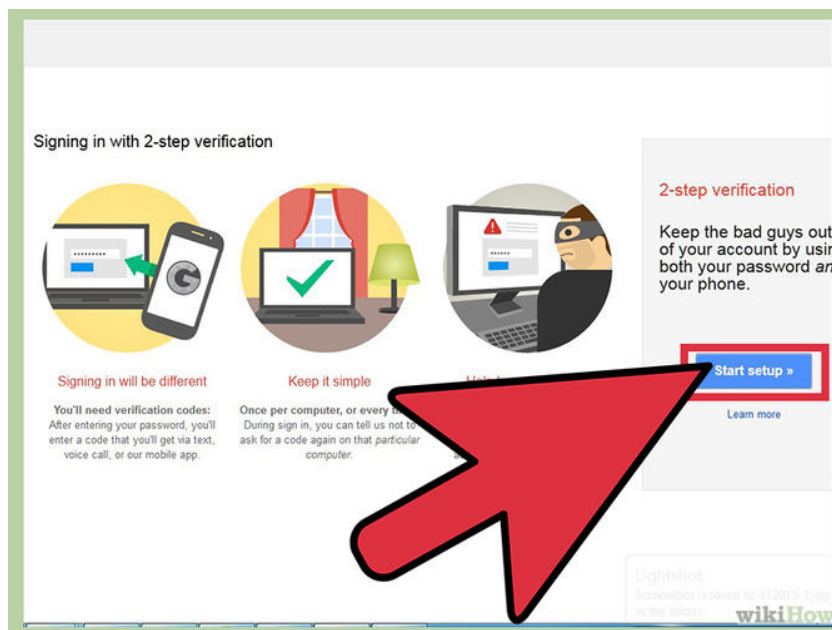
Step 2: You will land on your Account Settings page. Scroll down until you find a blue bar that says "signing in".



Step 3: In the 2-step verification section, you'll see if you already have 2-step verification turned on. If it says "OFF," click "Edit" to set the feature up.



Step 4: You'll see a page that briefly walks through the steps of setting up 2-step verification. Hover over the steps for more detail. Once you're ready, click "Start setup."



Step 5: Type in your cell phone number. This will be the phone associated with your Google account. Anytime you sign into your Google account from an unknown device (e.g., a public computer), Google will send a verification code to your phone and you will need to enter that before you can sign in.

Set up your phone

1 2 3 4

Which phone should we send codes to?

Google will send a numeric code to your phone whenever you sign in from an untrusted computer or device.

Phone number ex: (201) 555-5555

How should we send you

☒ Text message (SMS)

☐ Voice Call

[Back](#) [Send code](#)

wikiHow

Step 6: Select whether you'd like to receive a text message or Google Voice call with your verification code. Press submit. Then wait for the code to arrive to your phone and enter it in.

Verify your phone

1 2 3

We sent a text message to [redacted] with a code

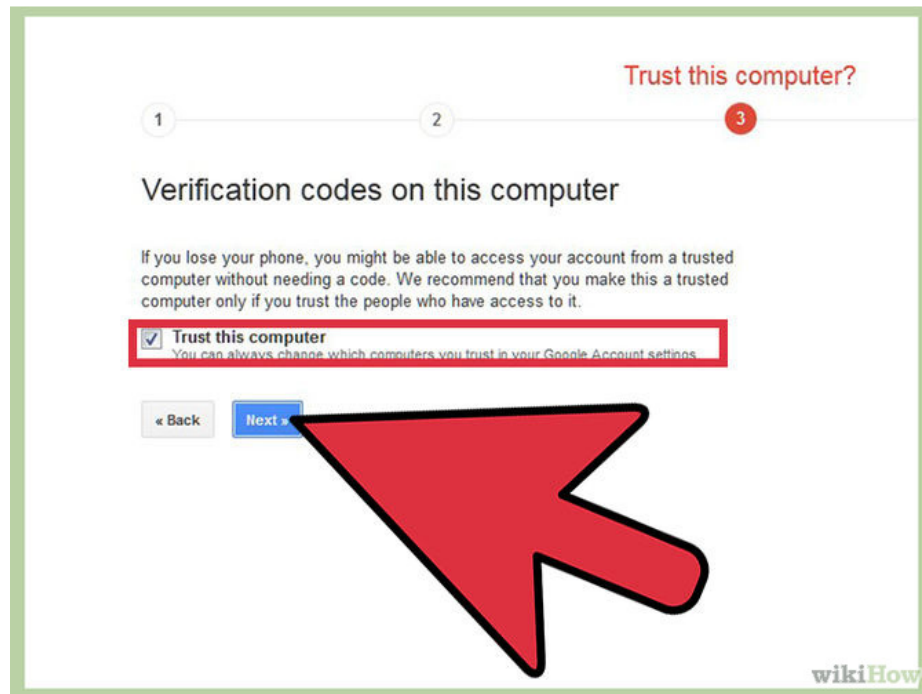
Enter verification code

Verification codes are 6 digits long.

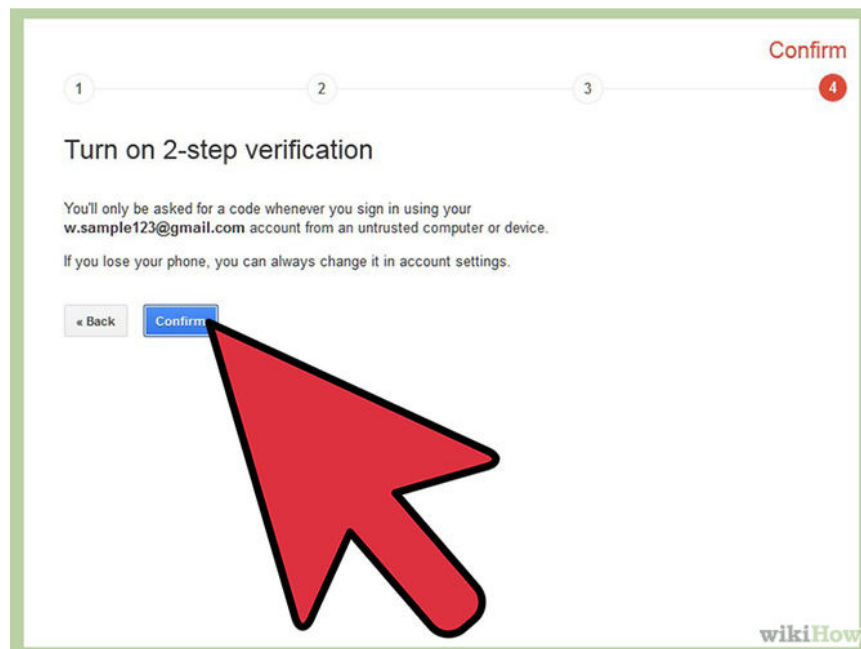
[Back](#) [Verify](#) [Didn't get the code](#)

wikiHow

Step 7: Decide whether to trust this device. If you are turning on 2-step verification from a personal computer or trusted device, check the "trust this device" box. You will only be asked to enter a verification code when you sign into this account once per 30 days.

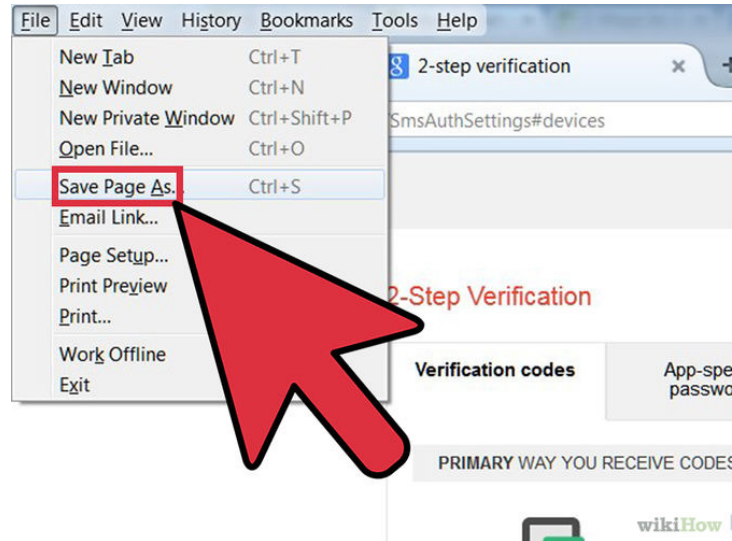


Step 8: Press OK, and you have just set up 2-step verification for your Google account! Skip any additional steps that seem unfamiliar or confusing for now -- we will address all of them in successive sections of this article.

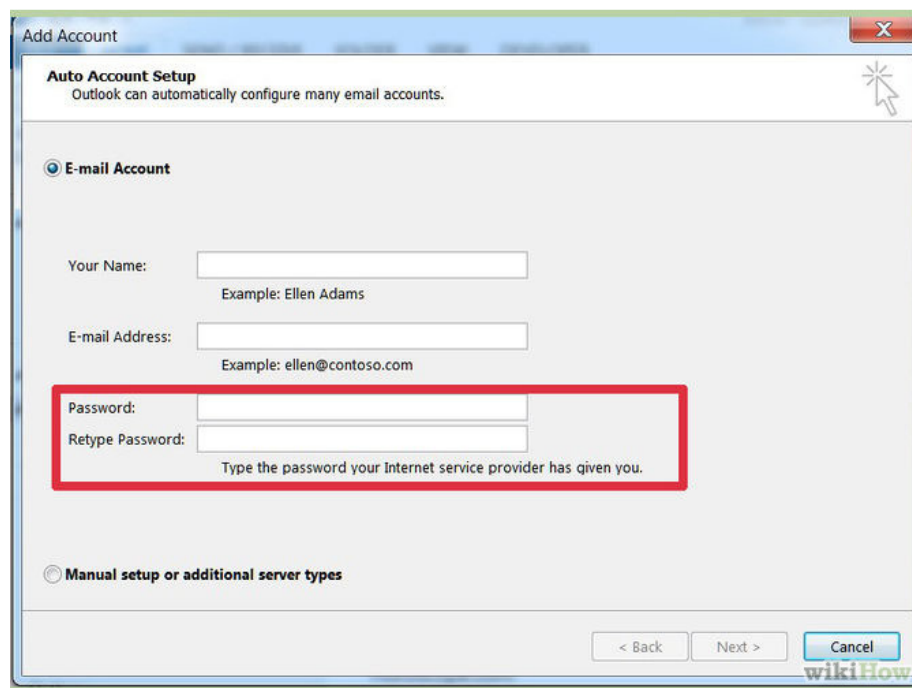


Step 9: Print a list of backup verification codes and store it in a secure but accessible place, like your wallet. If you ever need to sign into your Google account but don't have your primary phone with you, you can enter one of these codes instead.

- Go to your 2-step verification settings page.
- Under "How to receive codes," click on the "Show backup codes" link. Print this page.

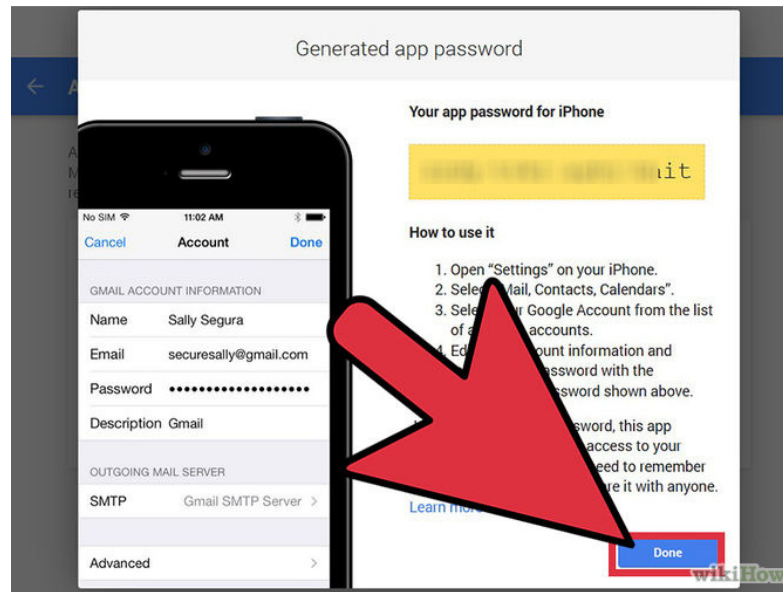


Method 1 of 2: Application-Specific Passwords

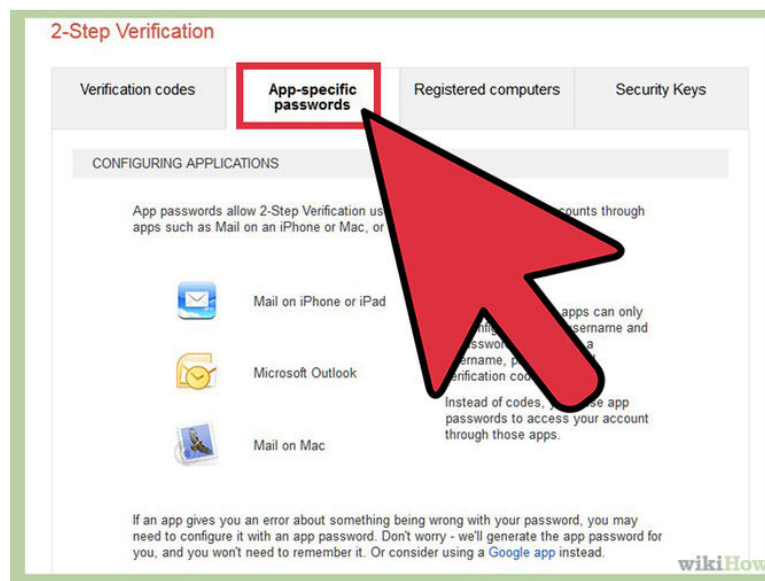


Step 1: Understand the need for application-specific passwords. With 2-step verification, Google has you covered every time you sign into your account from a web browser. However, if you use your Google account with other applications, such as Microsoft Outlook

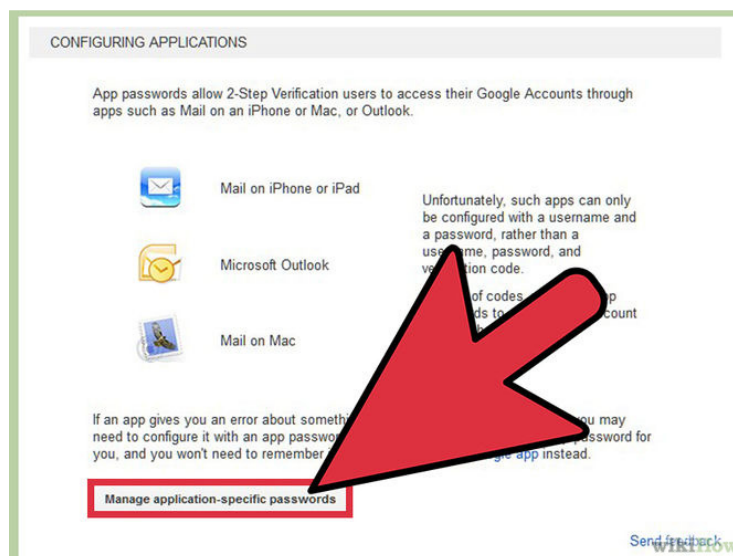
or a mobile device's mail application, those systems cannot ask you for a verification code. Therefore, you will need to sign into those systems *once* with an application-specific password. You will only need to re-enter an application-specific password if you choose to reset it and generate a new one for that device.



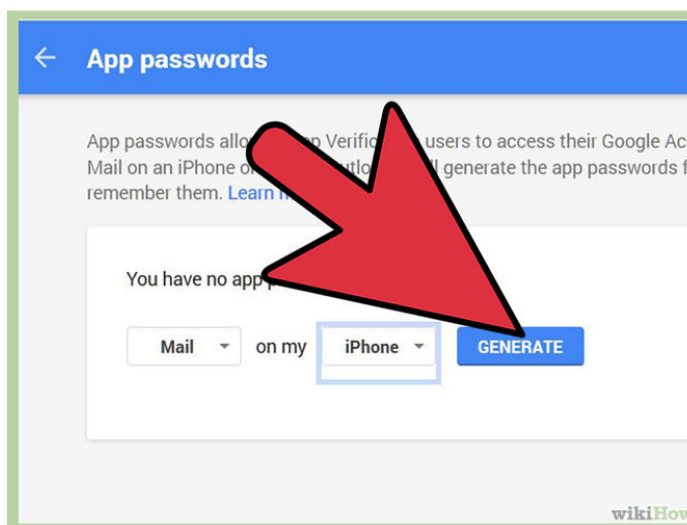
Step 2: Generate application-specific passwords for your devices. Go to your 2-step verification settings page or click "Edit" next to 2-step verification on the Security Account Settings page (steps 1-3 above). Scroll down and click on "Manage application-specific passwords."



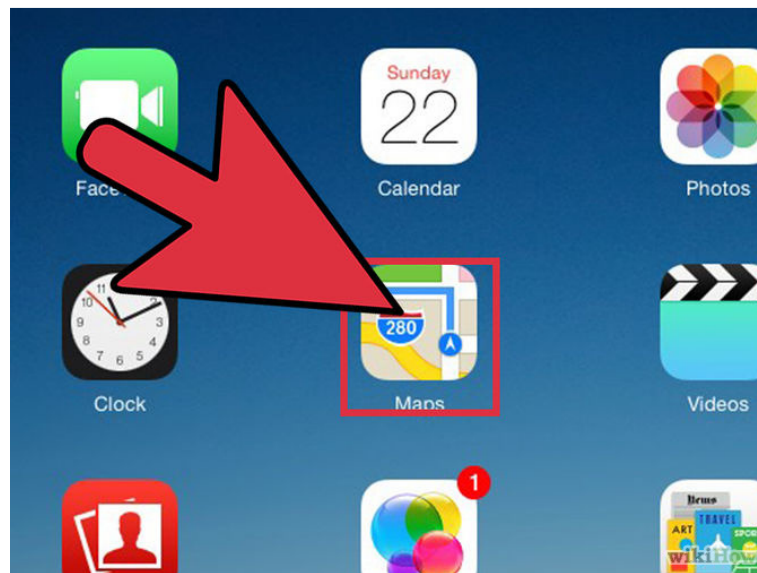
Step 3: At the top of the page, you will see a list of sites, applications and devices to which you have granted some level of access to your account. If you allowed a third-party website (e.g., LinkedIn, Twitter, Foursquare) to comb your Gmail Contacts to find friends, for example, you will see that listed. If you use other Google applications, you will also see those listed. Feel free to revoke access to any site or program you no longer wish to use.



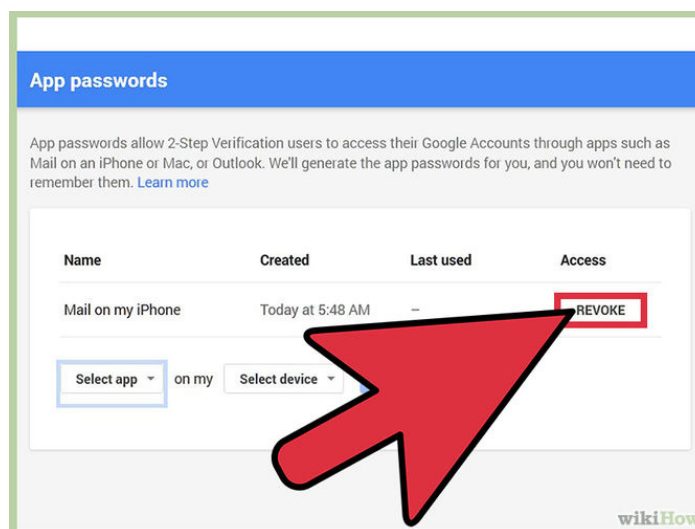
Step 4: Scroll down to the field at the bottom for entering the name of a device. Enter in something that will help you remember what this application-specific password is for -- e.g., Mail App on iPhone, Google App on iPhone, Chrome Sync, Outlook, Thunderbird, or whatever describes your application. Click "Generate password". You should generate a new application-specific password for *each* application.



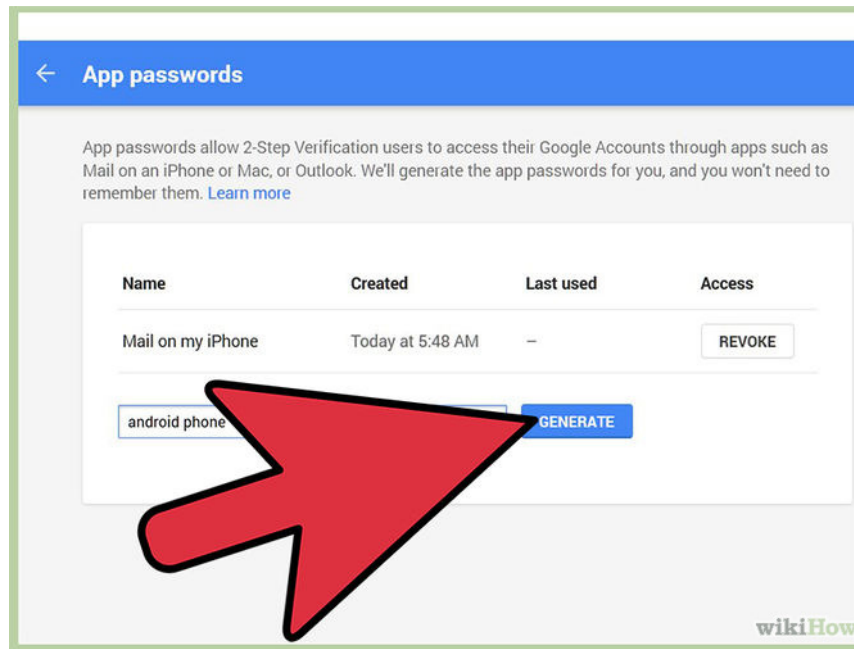
Step 5: Open up the application. Go to the settings page where you enter in your Google Account information. Type in your Google account name as usual. Now instead of your account password, type in the application-specific password in the password field. You have now granted this application full access to your Google account. You will only need to enter this password once. There is no need to write it down or memorize it, and it will not be displayed by Google again.



Step 6: Click "Done" on your web browser once you have successfully entered the application-specific password.



Step 7: Know how to revoke an app's access to your Gmail account. If you don't want to use an app anymore, or you lost your phone and want to stop anyone who has it from accessing your Gmail, simply click on the "Revoke" button in your application-specific password settings page.



Step 8: Create new application-specific passwords for *each* application that you connect your Google Account to! This means if you sync your Google Account to two mail apps and a chat client, you should have *three* application-specific passwords.

Method 2 of 2: If You Lose Your Phone

If you lose your phone and have 2-step verification turned on, you *can* still access your Gmail account. You also can and should follow these steps to stop strangers from gaining access to your Google accounts.

Step 1: Revoke your current application-specific passwords. If you have a smartphone with apps linked to your Google account, they will automatically be signed out. When you get a new phone, you can generate new application-specific passwords (see previous section) and enter them into your new devices.

Step 2: Change your Gmail password. Even if someone else has your verification code, they can't get into your Gmail account without your new password. While it's unlikely that the person who has your phone also has cracked your Gmail password, you can never be too

sure. If you are logged into Google from any web browser on your mobile device, you'll now also automatically be signed out.

Step 3: Add a backup phone number if you have a second mobile device. Go to your 2-step verification settings page and click "Add a phone number" in the "Backup phones" section.

Step 4: If you don't have a backup phone, use your list of printable backup codes to access your account. On your 2-step verification settings page, click "Show backup codes". If you haven't done so already, print out this page and keep it in a safe but accessible place -- such as your wallet.

Step 5: If you get phone and change your phone number, be sure to revoke access to your previous number on the 2-step verification settings page.

Activities

1. Use the guidelines to for generating secure passwords and evaluate whether your current passwords can be considered as safe or unsafe passwords.
2. Based on the above guidelines, change your unsafe passwords to safe ones.
3. Find out some popular password managers and evaluate them based on their characteristics'.
4. Based on the above comparison, choose one of the best password managers for yourself.
5. Create two step verification for your Gmail account.
6. Find out how many sites, other than Gmail provide two steps verification.

RECOMMENDED VIDEO:

https://youtu.be/Xhmae4_fG2o

<https://youtu.be/COU5T-Wafa4>

<https://youtu.be/cUH3tQbGj4A>

<https://youtu.be/hYyWgPXfx9U>

UNIT II: Firewall

1.3 CONFIGURING FIREWALL IN YOUR COMPUTER

1.3.1 How to Configure Your Mac's Firewall⁴

Every Mac ships with a built-in firewall - a service that can be configured to disallow information from entering your Mac. But what is a firewall, and why do you need to use it on your Mac?

Every time you request information from the Internet, such as a web page or email message, your Mac sends data packets to request the information. Servers receive the packets, and then send other packets back to your Mac. This all happens in a matter of seconds. Once your Mac has reassembled the packets, you'll see something, like an email message or web page.

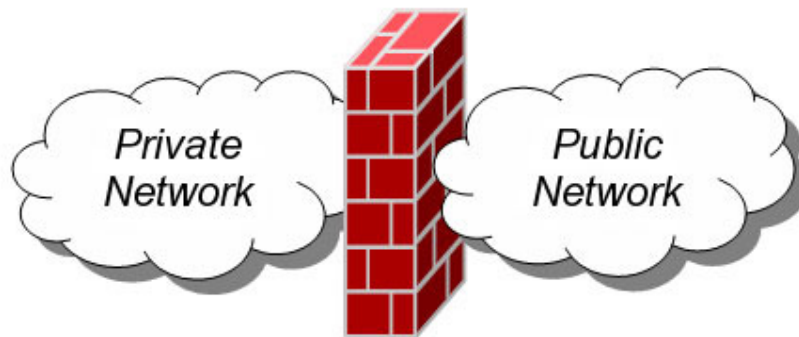


Figure 6: Firewall

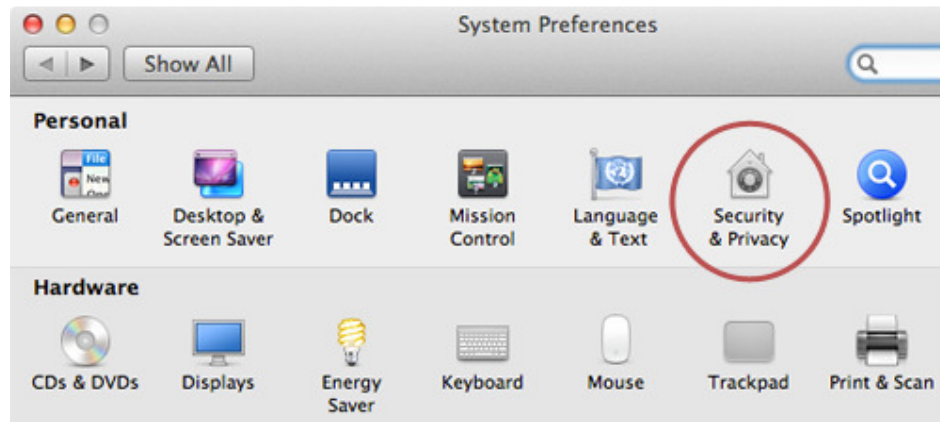
A firewall can help prevent bad packets from entering your Mac. Hackers love to run automated applications that can scan thousands of computers (including your Mac) for open ports that can be exploited. To ensure that random individuals do not gain unauthorized access to your Mac, you should enable Mac OS X's built-in firewall. It will close your Mac's open ports and disallow random network scans.

1.3.1.1 Turning on and Configuring the Mac OS X Firewall

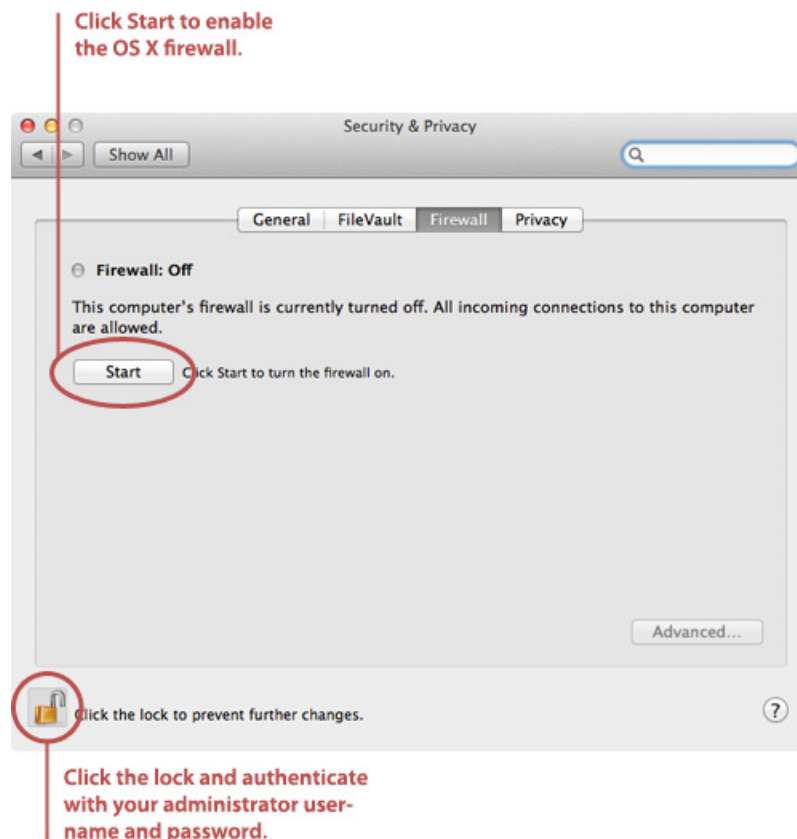
Here's how to turn on and configure your Mac's built-in firewall:

1. From the Apple menu, select **System Preferences**. The window shown below appears.

⁴ <http://www.macinstruct.com/node/165>



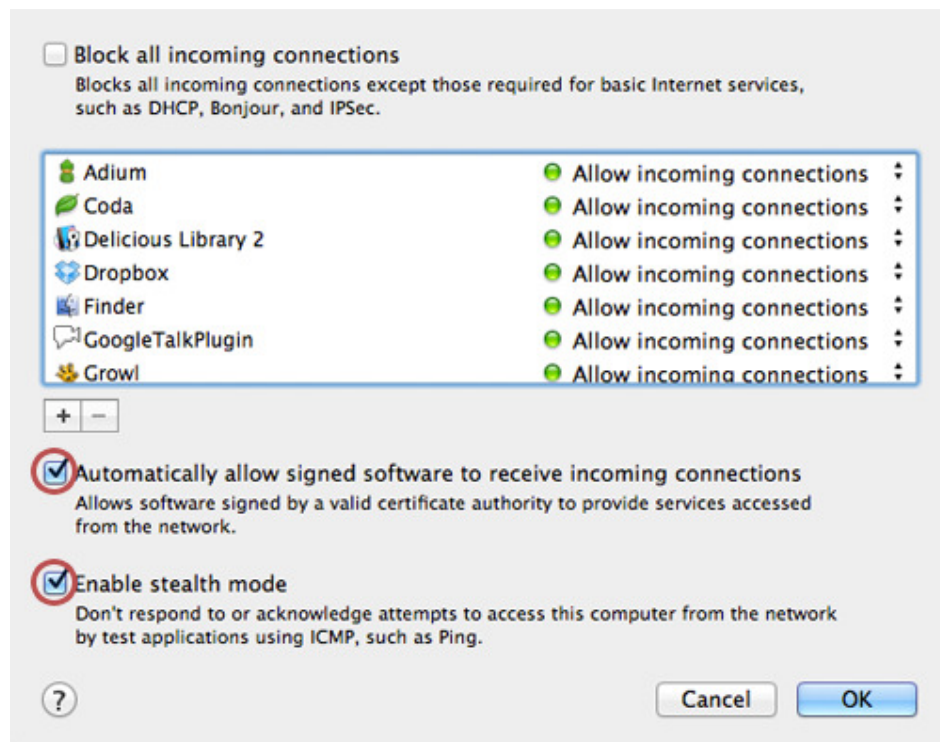
2. Select **Security & Privacy**.
3. Click the **Firewall** tab.
4. Click the lock icon and authenticate with your administrator username and password. The window shown below appears.



5. Click **Start**. The firewall turns on - you'll know it's enabled when you see the green light and the **Firewall: On** message, as shown below.



6. Click **Advanced**. The window shown below appears.



7. Select the **Automatically allow signed software to receive incoming connections** checkbox. This allows the applications on your Mac to communicate with the outside world.
8. Select the **Enable stealth mode** checkbox. This prevents your Mac from responding to port scans and ping requests.
9. Click **OK** to close the *Advanced* settings.
10. Close System Preferences. Your Mac is now protected by the built-in firewall!

1.3.2 Working with Windows Firewall in Windows 7⁵

1.3.2.1 Firewall in Windows 7

Windows 7 comes with two firewalls that work together. One is the **Windows Firewall**, and the other is **Windows Firewall with Advanced Security (WFAS)**. The main difference between them is the complexity of the rules configuration. Windows Firewall uses simple rules that directly relate to a program or a service. The rules in WFAS can be configured based on protocols, ports, addresses and authentication. By default, both firewalls come with predefined set of rules that allow us to utilize network resources. This includes things like browsing the web, receiving e-mails, etc. Other standard firewall exceptions are File and Printer Sharing, Network Discovery, Performance Logs and Alerts, Remote Administration, Windows Remote Management, Remote Assistance, Remote Desktop, Windows Media Player, Windows Media Player Network Sharing Service.

With firewall in Windows 7 we can configure inbound and outbound rules. By default, all outbound traffic is allowed, and inbound responses to that traffic are also allowed. Inbound traffic initiated from external sources is automatically blocked.

Sometimes we will see a notification about a blocked program which is trying to access network resources. In that case we will be able to add an exception to our firewall in order to allow traffic from the program in the future.

Windows 7 comes with some new features when it comes to firewall. For example, "full-stealth" feature blocks other computers from performing operating system fingerprinting. OS fingerprinting is a malicious technique used to determine the operating system running on the host machine. Another feature is "boot-time filtering". This feature ensures that the firewall is working at the same time when the network interface becomes active, which was not the case in previous versions of Windows.

When we first connect to some network, we are prompted to select a network location. This feature is known as Network Location Awareness (NLA). This feature enables us to assign a network profile to the connection based on the location. Different network profiles contain different collections of firewall rules. In Windows 7, different network profiles can be configured on different interfaces. For example, our wired interface can have different profile than our wireless interface. There are three different network profiles available:

- Public

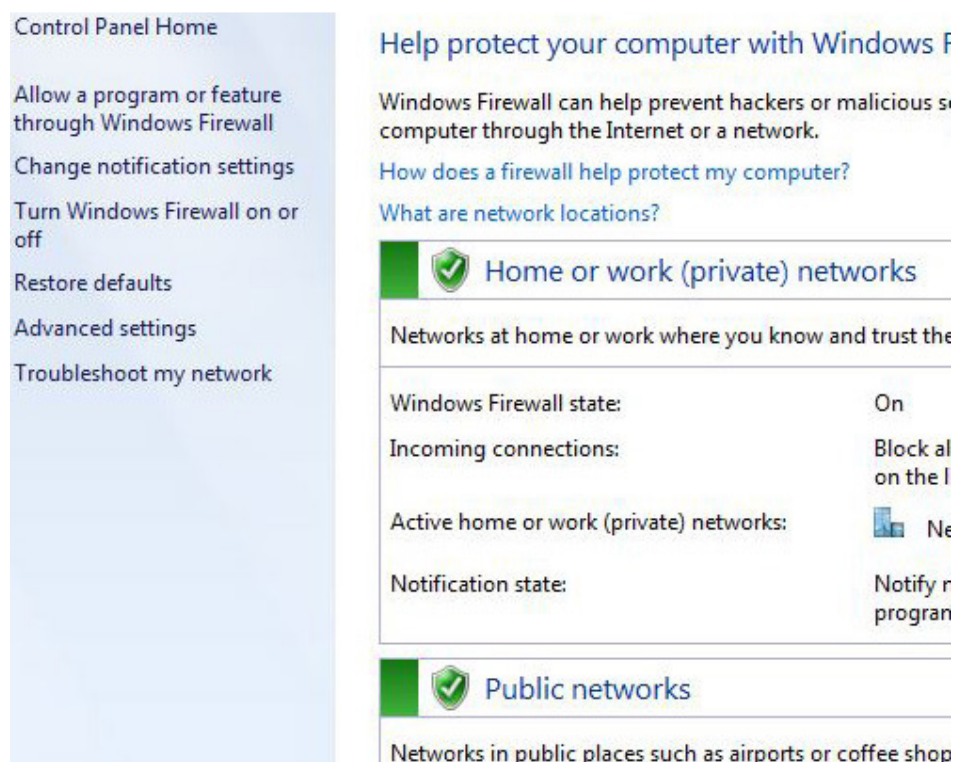
⁵ <http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-in-windows-7>

- Home/Work - private network
- Domain - used within a domain

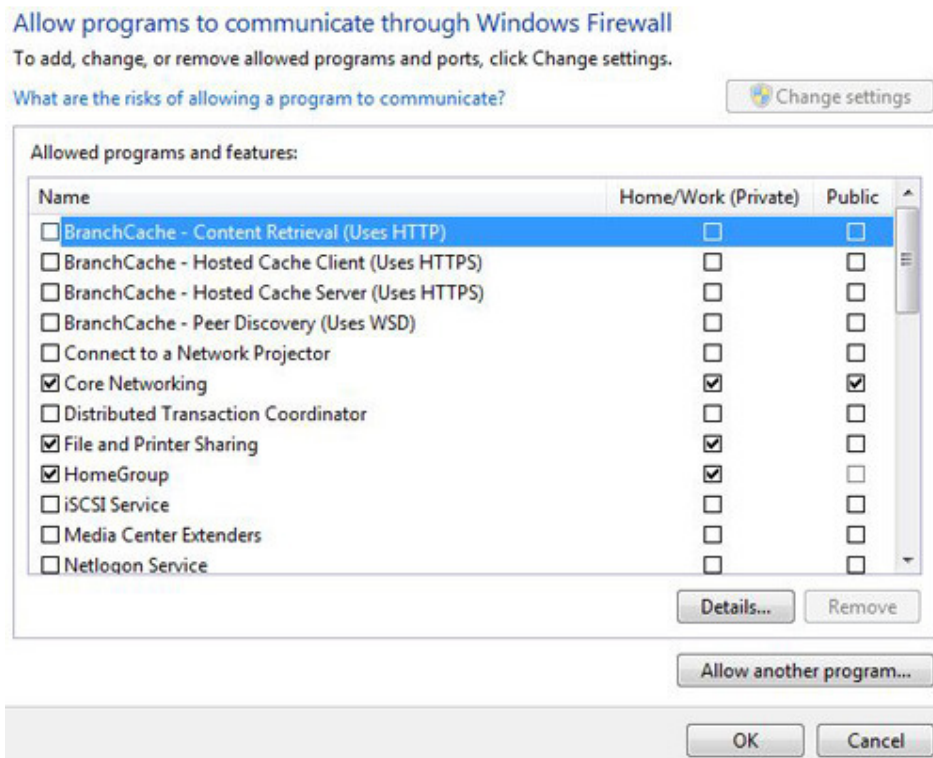
We choose those locations when we connect to a network. We can always change the location in the Network and Sharing Center, in Control Panel. The Domain profile can be automatically assigned by the NLA service when we log on to an Active Directory domain. Note that we must have administrative rights in order to configure firewall in Windows 7.

1.3.2.2 Configuring Windows Firewall

To open Windows Firewall we can go to **Start > Control Panel > Windows Firewall**.

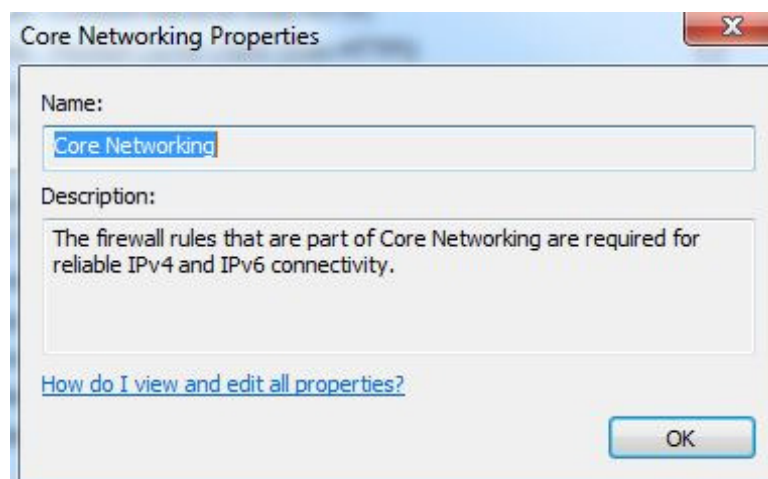


By default, Windows Firewall is enabled for both private (home or work) and public networks. It is also configured to block all connections to programs that are not on the list of allowed programs. To configure exceptions we can go to the menu on the left and select "Allow a program or feature through Windows Firewall" option.



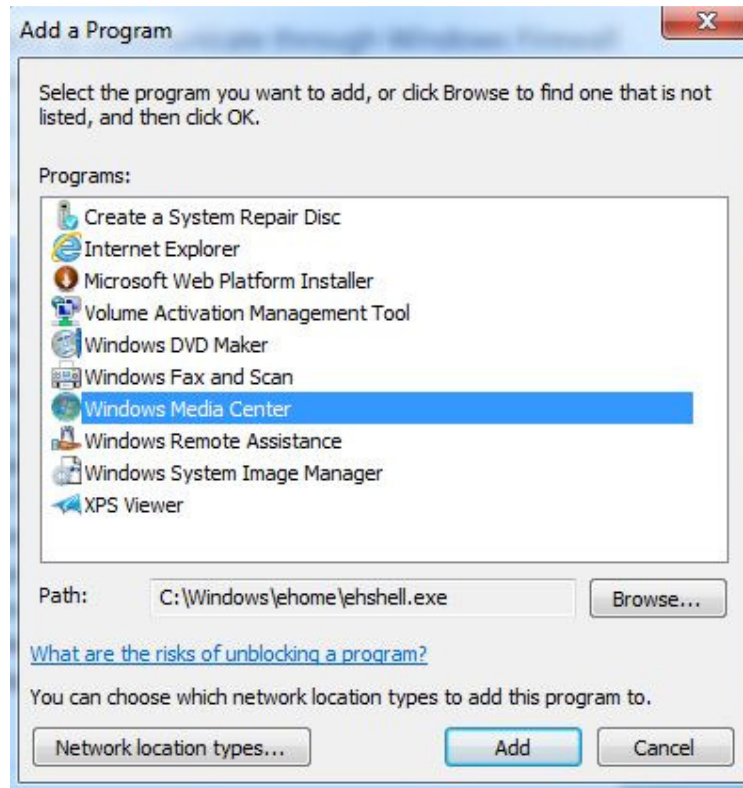
Exceptions

To change settings in this window we have to click the "Change settings" button. As you can see, here we have a list of predefined programs and features that can be allowed to communicate on private or public networks. For example, notice that the Core Networking feature is allowed on both private and public networks, while the File and Printer Sharing is only allowed on private networks. We can also see the details of the items in the list by selecting it and then clicking the Details button.



Details

If we have a program on our computer that is not in this list, we can manually add it by clicking on the "Allow another program" button.



Add a Program

Here we have to browse to the executable of our program and then click the Add button. Notice that we can also choose location types on which this program will be allowed to communicate by clicking on the "Network location types" button.



Network Locations

Many applications will automatically configure proper exceptions in Windows Firewall when we run them. For example, if we enable streaming from Media Player, it will automatically configure firewall settings to allow streaming. The same thing is if we enable Remote Desktop feature from the system properties window. By enabling Remote Desktop feature we actually create an exception in Windows Firewall.



Windows Firewall can be turned off completely. To do that we can select the "Turn Windows Firewall on or off" option from the menu on the left.

Customize settings for each type of network



You can modify the firewall settings for each type of network location that you use.

[What are network locations?](#)

Home or work (private) network location settings

-  ☒ Turn on Windows Firewall
 - ☐ Block all incoming connections, including those in the list of allowed programs
 - ☒ Notify me when Windows Firewall blocks a new program
-  ☐ Turn off Windows Firewall (not recommended)

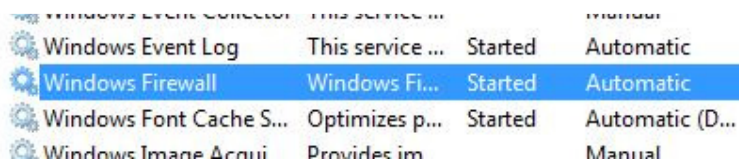
Public network location settings

-  ☒ Turn on Windows Firewall
 - ☐ Block all incoming connections, including those in the list of allowed programs
 - ☒ Notify me when Windows Firewall blocks a new program
-  ☐ Turn off Windows Firewall (not recommended)

Firewall Customization

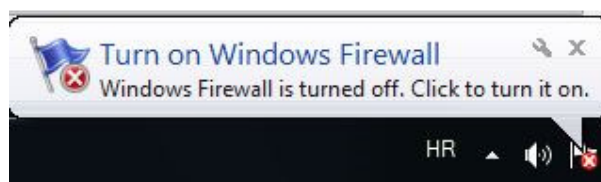
Note that we can modify settings for each type of network location (private or public). Interesting thing here is that we can block all incoming connections, including those in the list of allowed programs.

Windows Firewall is actually a Windows service. As you know, services can be stopped and started. If the Windows Firewall service is stopped, the Windows Firewall will not work.



Firewall Service

In our case the service is running. If we stop it, we will get a warning that we should turn on our Windows Firewall.



Warning

Remember that with Windows Firewall we can only configure basic firewall settings, and this is enough for most day-to-day users. However, we can't configure exceptions based on ports in Windows Firewall any more. For that we have to use Windows Firewall with Advanced Security, which will be covered in next section.

1.3.3 How to Start & Use The Windows Firewall with Advanced Security⁶

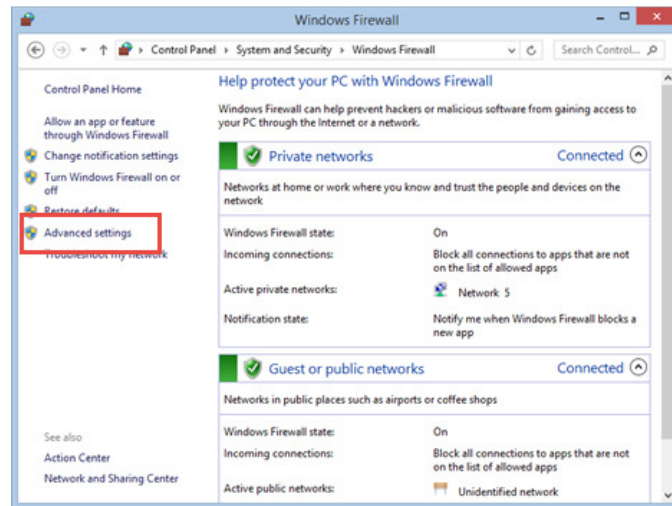
The *Windows Firewall with Advanced Security* is a tool which gives you detailed control over the rules that are applied by the *Windows Firewall*. You can view all the rules that are used by the *Windows Firewall*, change their properties, create new rules or disable existing ones. In this tutorial we will share how to open the *Windows Firewall with Advanced Security*, how to find your way around it and talk about the types of rules that are available and what kind of traffic they filter.

1.3.3.1 How to Access the Windows Firewall with Advanced Security

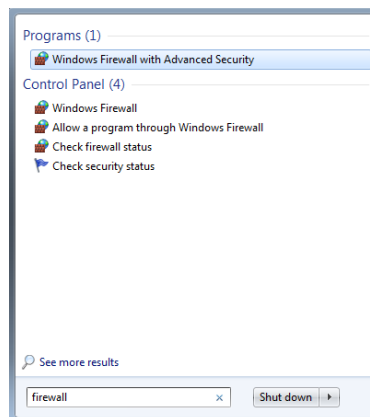
You have several alternatives to opening the *Windows Firewall with Advanced Security*:

One is to open the standard Windows Firewall window, by going to "Control Panel -> System and Security -> Windows Firewall". Then, click or tap *Advanced settings*.

⁶ <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security>

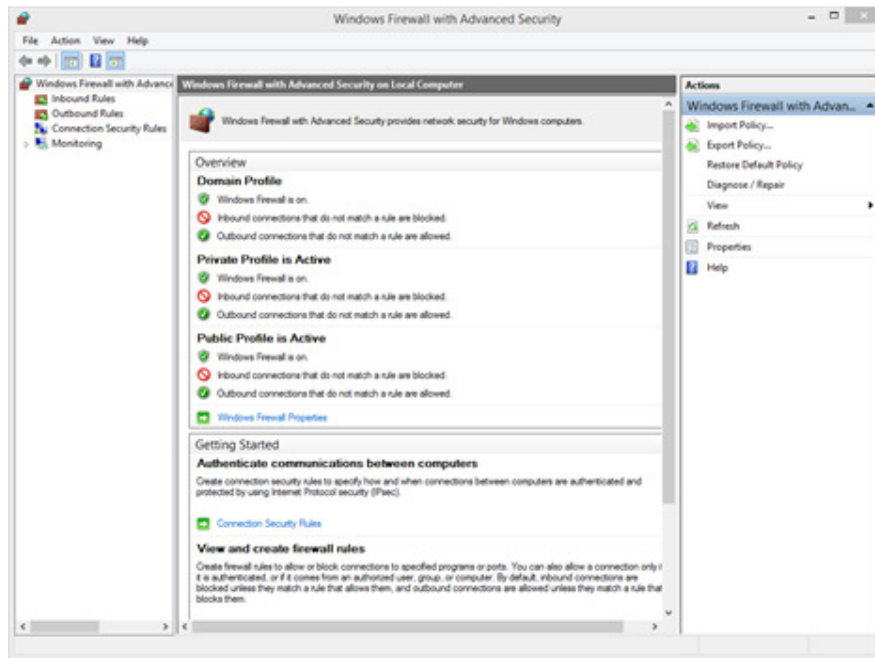


In Windows 7, another method is to search for the word *firewall* in the *Start Menu* search box and click the "*Windows Firewall with Advanced Security*" result.



In Windows 8.1, *Windows Firewall with Advanced Security* is not returned in search results and you need to use the first method shared above for opening it.

The *Windows Firewall with Advanced Security* looks and works the same both in Windows 7 and Windows 8.1. To continue our tutorial, we will use screenshots that were made in Windows 8.1.



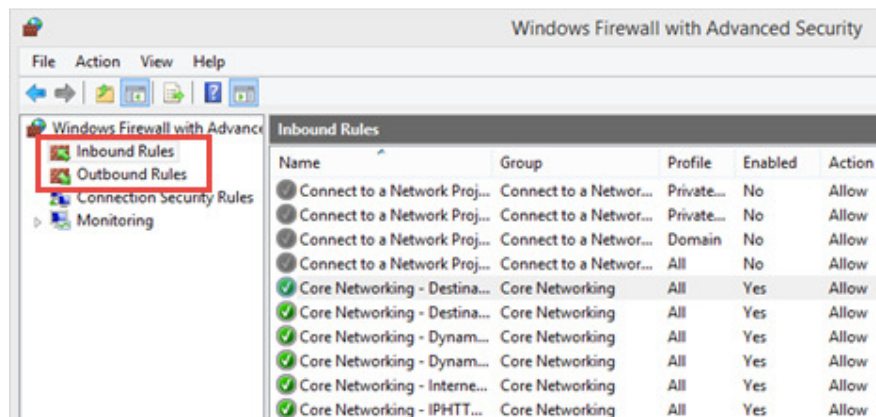
1.3.3.2 What Are The Inbound & Outbound Rules?

In order to provide the security you need, the *Windows Firewall* has a standard set of inbound and outbound rules, which are enabled depending on the location of the network you are connected to.

Inbound rules are applied to the traffic that is coming from the network and the Internet to your computer or device. Outbound rules apply to the traffic from your computer to the network or the Internet.

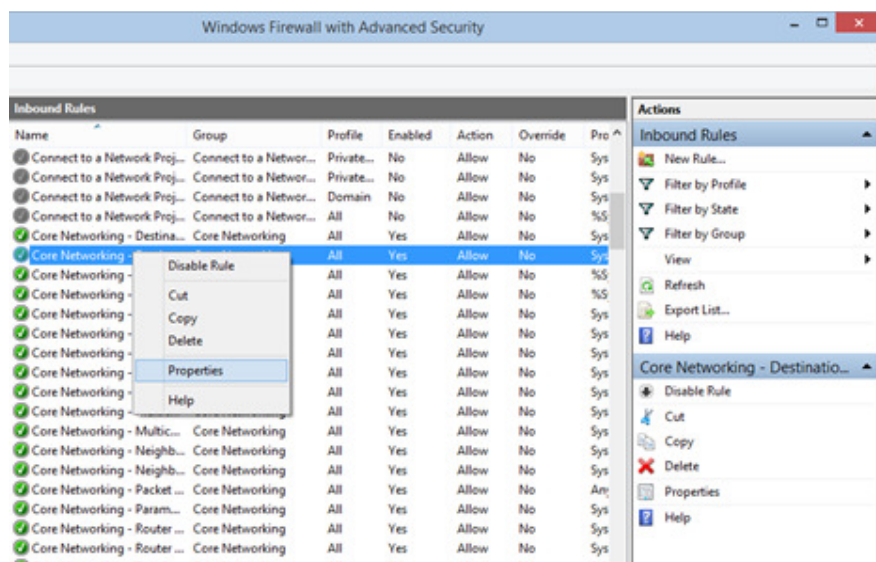
These rules can be configured so that they are specific to: computers, users, programs, services, ports or protocols. You can also specify to which type of network adapter (e.g. wireless, cable, virtual private network) or user profile it is applied to.

In the *Windows Firewall with Advanced Security*, you can access all rules and edit their properties. All you have to do is click or tap the appropriate section in the left-side panel.

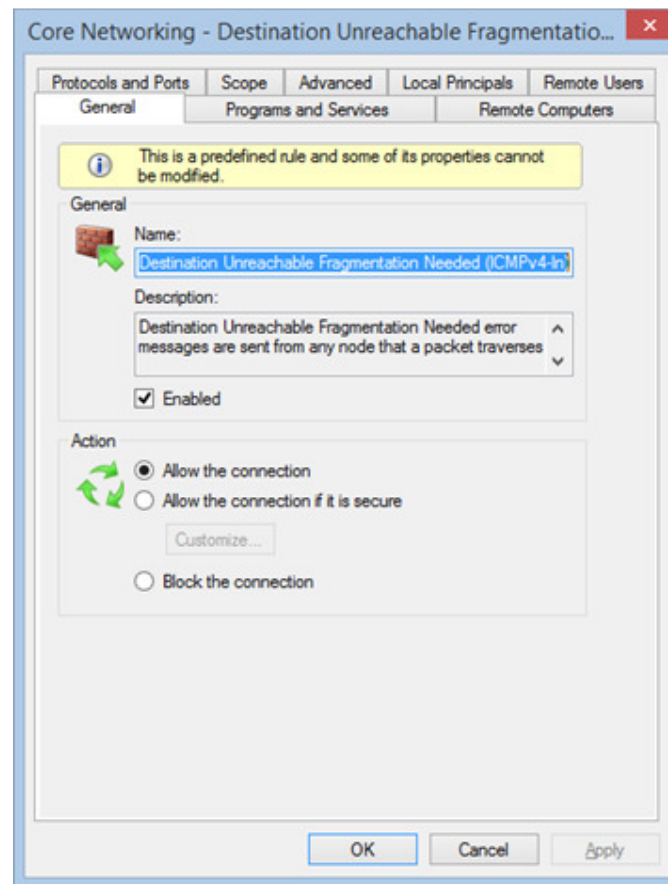


The rules used by the *Windows Firewall* can be enabled or disabled. The ones which are enabled or active are marked with a green check-box in the *Name* column. The ones that are disabled are marked with a gray check-box.

If you want to know more about a specific rule and learn its properties, right click on it and select *Properties* or select it and press *Properties* in the column on right, which lists the actions that are available for your selection.



In the *Properties* window, you will find complete information about the selected rule, what it does and in when it is applied. You will also be able to edit its properties and change any of the available parameters.

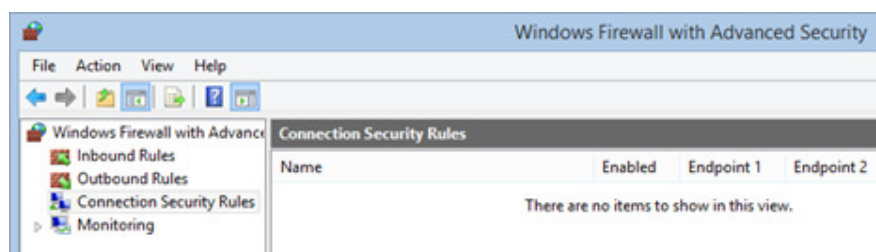


1.3.3.3 What Are The Connection Security Rules?

Connection security rules are used to secure traffic between two computers while it crosses the network. One example would be a rule which defines that connections between two specific computers must be encrypted.

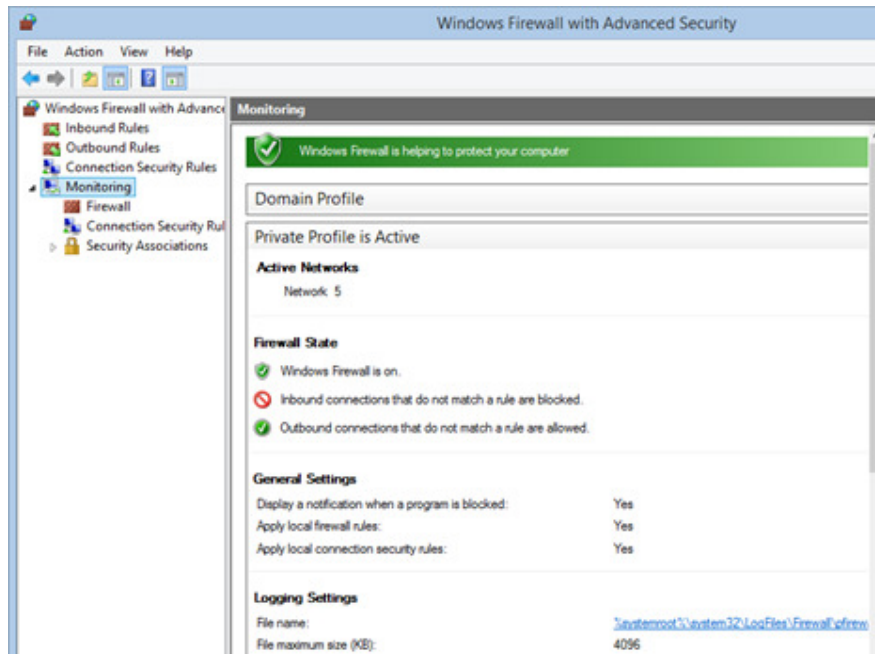
Unlike the inbound or outbound rules, which are applied only to one computer, connection security rules require that both computers have the same rules defined and enabled.

If you want to see if there are any such rules on your computer, click or tap "Connection Security Rules" on the panel on the left. By default, there are no such rules defined on Windows computers and devices. They are generally used in business environments and such rules are set by the network administrator.



1.3.3.4 What Does the Windows Firewall with Advanced Security Monitor?

The *Windows Firewall with Advanced Security* includes some monitoring features as well. In the *Monitoring* section you can find the following information: the firewall rules that are active (both inbound and outbound), the connection security rules that are active and whether there are any active security associations.



You should note that the *Monitoring* section shows only the active rules for the current network location. If there are rules which get enabled for other network locations, you will not see them in this section.

The above section discussed on how to setup a firewall on two Operating Systems viz. Windows and Mac. Linux have many variants therefore it is not possible to discuss how to configure firewall on Linux. There are some links in the Recommended Videos section which discuss the procedure of setting up firewall in various variant of Linux.

Activity

1. Setup and configure a firewall in your system.
2. Find some of the free and commercially available firewalls over internet.

RECOMENDED VIDEOS

<https://www.youtube.com/watch?v=krbivwp4t3U>

<https://www.youtube.com/watch?v=H0g8xJMnT68>

For linux

<https://www.youtube.com/watch?v=hkzHtEnFZpc>

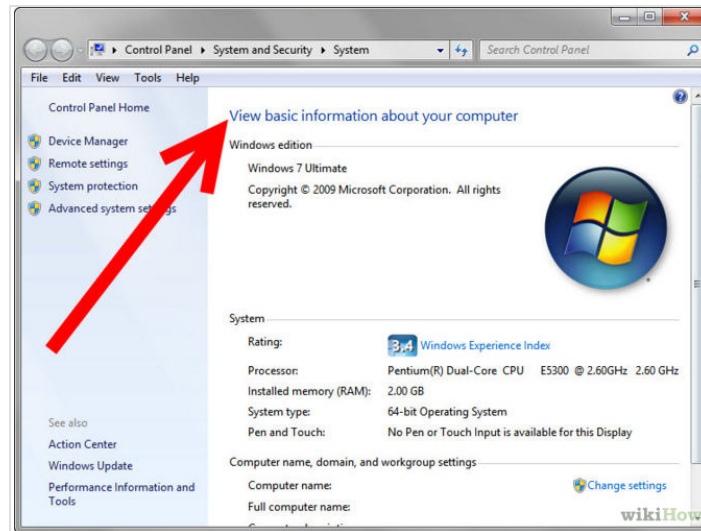
https://www.youtube.com/watch?v=o0a09CQi_48

<https://www.youtube.com/watch?v=wbzP2-qvc4o>

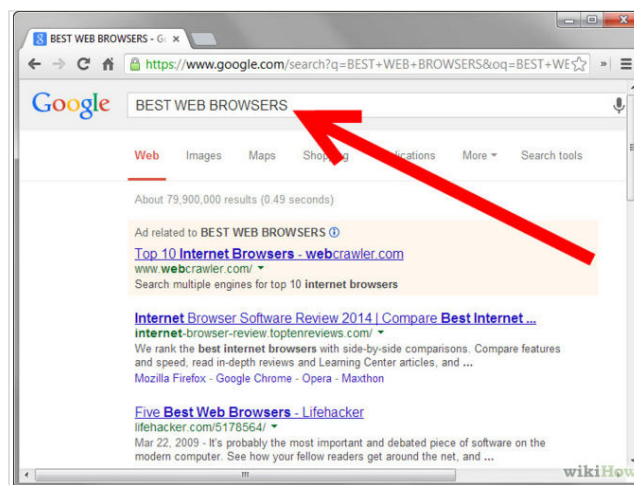
UNIT III: How to Choose an Internet Browser

1.4 STEPS TO FIND THE BEST BROWSER ACCORDING TO THE USERS REQUIREMENT⁷

Browsers are the key to the Internet these days, at least for most tasks. There are many, many browsers for every platform and operating system, so the choice can be tough. However, this should help narrow the search.

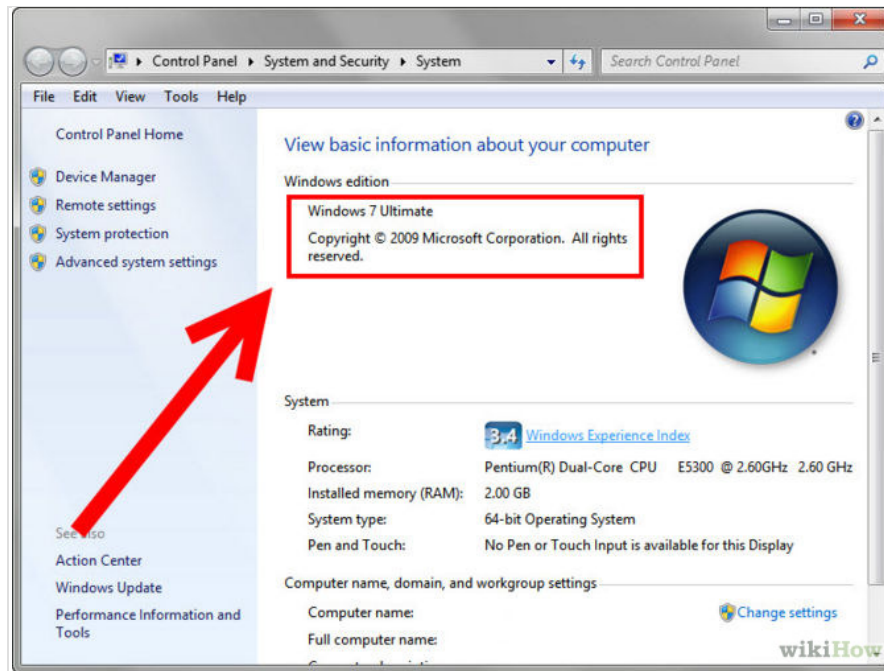


Step 1: Determine the age of your computer. How old is your computer? Is it a mobile device? Know your systems specifications as this may be more suited to some browsers than others.

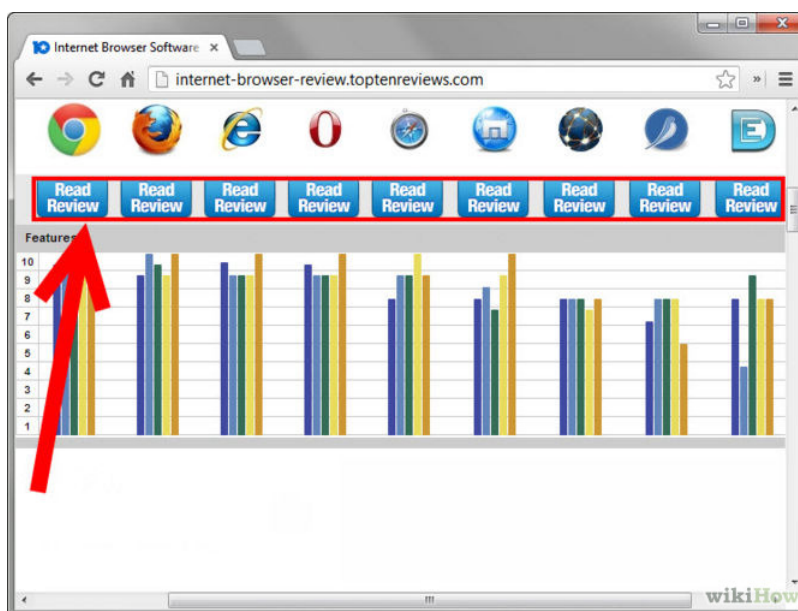


⁷ <http://www.wikihow.com/Choose-an-Internet-Browser>

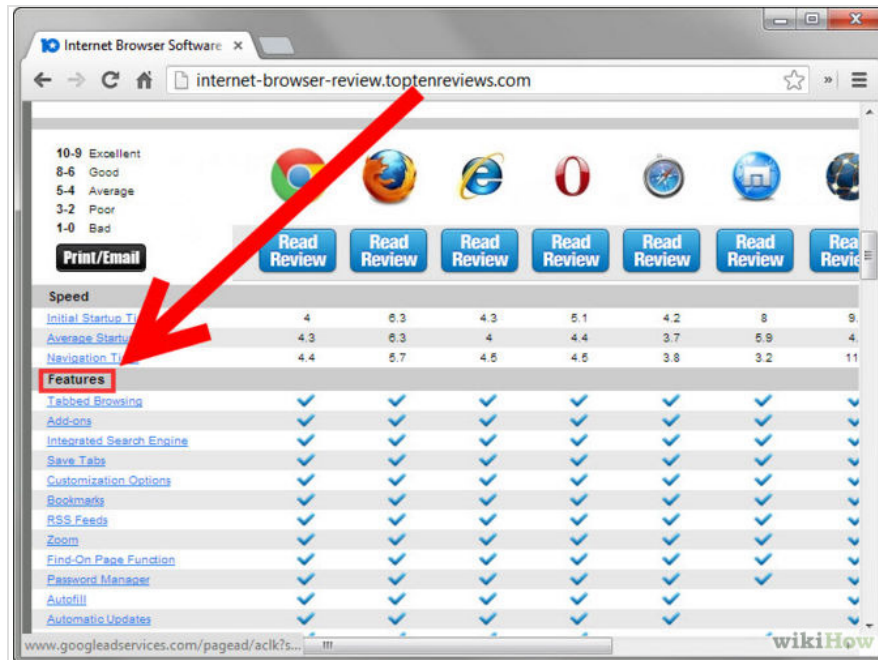
Step 2: Think about your ideal browser; what would it be able to do? You may want it to be quite simple, handling only the bare necessities. You may want some basic features like web feed reading, bookmarking (favorites), or search boxes. Some browsers have a lot more, and that's where it starts to get confusing.



Step 3: Make sure you know what platform you are on. Some browsers are only available to a certain operating system, or not available to one operating system.



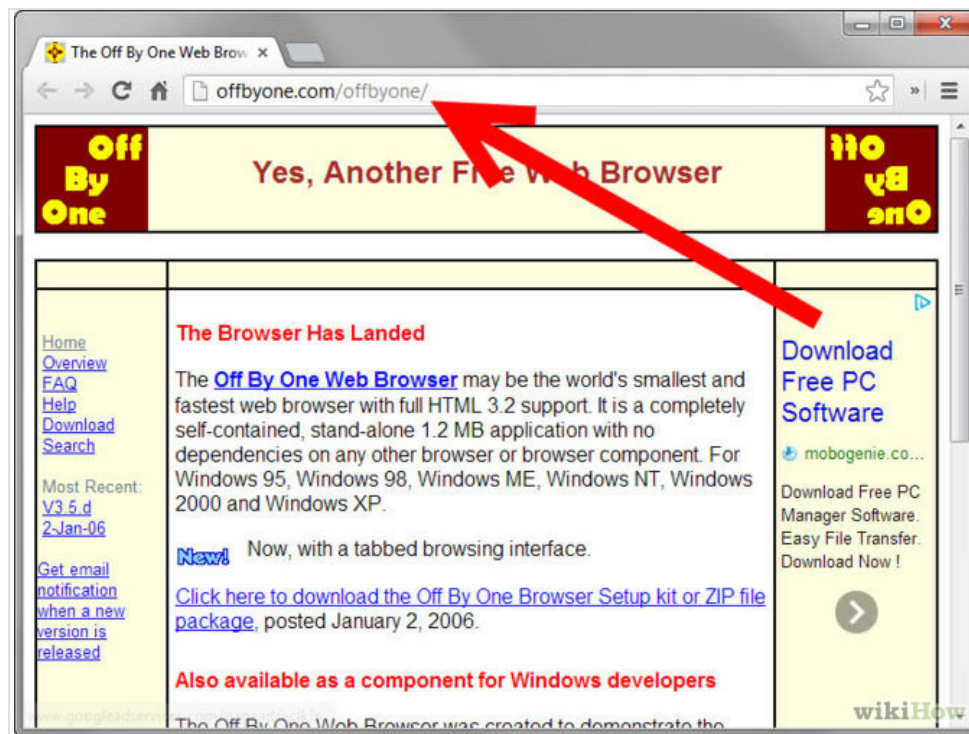
Step 4: Research browsers. Tabbed browsers include Safari (runs on OS X, iPhone and is new to Windows), Firefox (general purpose with the most plug-ins), Opera(supports torrents, handles e-mail and runs on mobile devices), Konqueror (dual purpose file manager), Seamonkey (includes HTML editor and e-mail client), Off By One (tiny) and Flock (social networking).



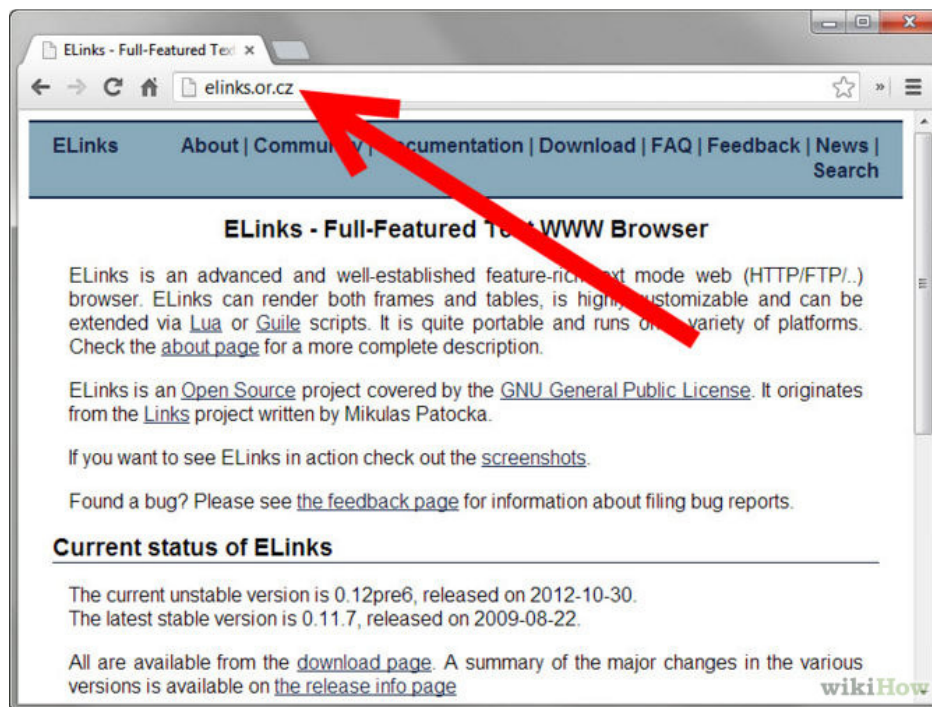
The screenshot shows a web browser window with the address bar displaying "internet-browser-review.toptenreviews.com". The page features a comparison table of various internet browsers. A red arrow points to the "Features" section of the table, which lists various browser features and their availability across different browsers.

Speed	4	6.3	4.3	5.1	4.2	8	9
Initial Startup Time	4	6.3	4.3	5.1	4.2	8	9
Average Startup Time	4.3	6.3	4	4.4	3.7	5.9	4
Navigation Time	4.4	5.7	4.5	4.5	3.8	3.2	11
Features							
Tabbed Browsing	✓	✓	✓	✓	✓	✓	✓
Add-ons	✓	✓	✓	✓	✓	✓	✓
Integrated Search Engine	✓	✓	✓	✓	✓	✓	✓
Save Tabs	✓	✓	✓	✓	✓	✓	✓
Customization Options	✓	✓	✓	✓	✓	✓	✓
Bookmarks	✓	✓	✓	✓	✓	✓	✓
RSS Feeds	✓	✓	✓	✓	✓	✓	✓
Zoom	✓	✓	✓	✓	✓	✓	✓
Find-On Page Function	✓	✓	✓	✓	✓	✓	✓
Password Manager	✓	✓	✓	✓	✓	✓	✓
Autofill	✓	✓	✓	✓	✓	✓	✓
Automatic Updates	✓	✓	✓	✓	✓	✓	✓

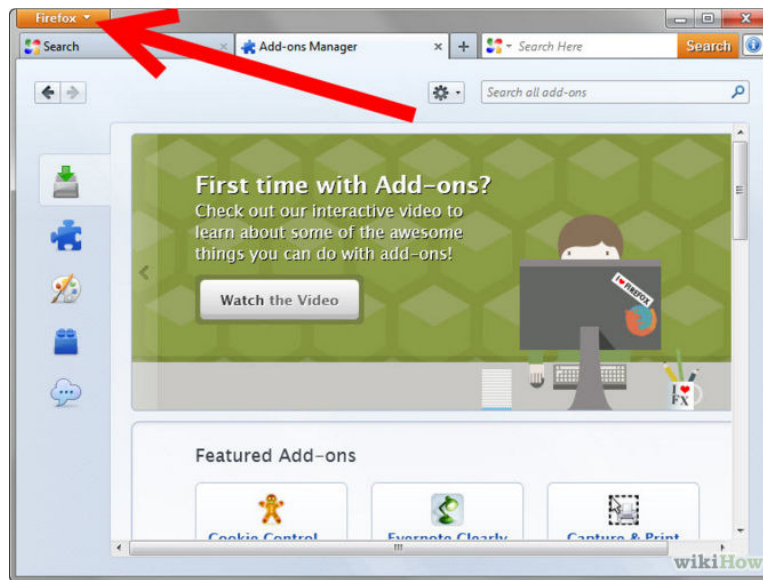
Step 5: See the features of all browsers you have found, and compare with what you want.



Step 6: Consider alternative lower-memory browsers, if you have low computer memory. Consider Off by One, Dillo, SkipStone and NetSurf.



Step 7: Consider a text-based browser, if you want an even faster-than-fast(maximum speed/hyperdrive) experience. Consider ELinks.



Step 8: Find out if you can add features you may want or if there is an easy method to doing so such as an existing plugin or extension in the case of Firefox.



Step 9: Download and install your new browser!

Activity

1. Compare the various browsers based on their characteristics’.

RECOMMENDED VIDEOS:

<https://www.youtube.com/watch?v=sr7mgYD2tAc>

<https://www.youtube.com/watch?v=-jHs-RYD7gc>

<https://www.youtube.com/watch?v=gNiz4kfSZnw>

UNIT IV: How to find out whether the website is safe to browse

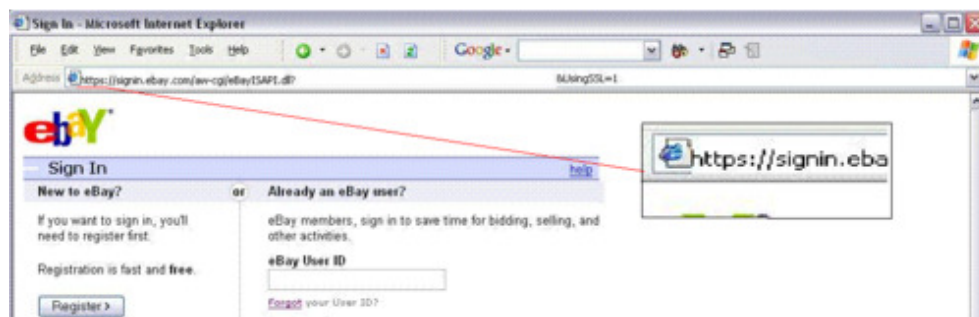
1.5 SAFE BROWSING

Internet security is a matter of great concern for internet users. It is important to **know if a website is secure** or not while surfing the internet⁸. A **secure website** creates a safe connection between the website and the web browser so that entered data, such as personal information, credit card details, banking information, etc, is not accessible to unauthorized entities. When the browser opens a secured connection, "https" can be seen in the URL instead of just http. To **know if a website is secure** or not, look for the locked yellow colored padlock symbol on the lower right corner of the browser window.

1.5.1 How do I know if a website is secure?

Some web sites use a secure connection between the web site and your browser. This may be important to you, for instance, if you want to pay online for a product or a service and have to enter credit card information or other personal information.

To know if your browser is viewing a secure web site, you can look in the lower right part of the window. There is a small box in the frame of the window to the left of the area that describes which zone you are in (usually the Internet zone, with a globe icon). If you see a yellow padlock icon, the web site you are viewing is a "secure web site." If the box is empty, the web site does not have a secure connection with your browser.



1.5.2 Tips for buying online⁹

⁸ <http://ccm.net/faq/2-how-do-i-know-if-a-website-is-secure>

⁹ <https://www.qld.gov.au/law/your-rights/consumer-rights-complaints-and-scams/consumer-advice-rights-and-responsibilities/tips-to-become-a-smarter-shopper/tips-for-buying-online/>

Shopping online can be cheaper and more convenient for you and for businesses. However, make sure you understand your rights and the risks before you shop online or bid in an online auction.

3. Pay securely: Don't make any payment unless:

- You are on a secure website, and
- You can make a secure payment.

This will protect you against fraud and unauthorised credit card transactions. A secure website address will always:

- begin with 'https://', not 'http://'
- display the image of a closed padlock (usually in the bottom right corner of your browser window).

Only make a payment if you can see both of these things. Never give out your bank account details, credit card number or other personal details if you are not certain that the business is a reputable trader.

4. Know the business: Only buy from websites you know and trust. Check that the company has a physical street address and landline phone number. If the company operates from overseas, you might have trouble getting a refund or repair.

5. Know the product: Make sure you check whether:

- the product is legal
- the product will work in Australia
- any warranties or guarantees offered are valid in Australia
- the product has an authorised repairer nearby.

6. Check the contract: Make sure you read and understand:

- the terms and conditions of sale
- the refund policy
- the delivery details
- returns and repairs policies, including any associated costs.

7. Check the full cost: Be aware of the full cost of your purchase. Additional costs may include:

- currency conversion
- taxes
- postage and delivery fees
- packaging.

It might end up being cheaper to buy the product at a local shop.

8. Protect your privacy

Only buy online if you are comfortable with a business's privacy policy. Do not give out information unless they require it to complete the sale. Remember, if a deal sounds too good to be true, it probably is.

9. Keep records

Always write down any reference numbers and print out copies of:

- the order form (both before and after you confirm the order)
- receipts (can come by email or in a pop-up window).

Always make sure all charges are correct by checking the receipt against your:

- credit card statement
- merchant account statement (such as PayPal)
- bank statement.

The charges may be converted from another currency.

10. Online auction sites

Most online auction sites (like eBay) offer a dispute resolution process for buyers and sellers.

This should be your first step to resolve a dispute if:

- you did not receive the items you bought
- you did not receive payment for items you sold
- you received items that were significantly different from their description.

The eBay website has an example of this facility.

Activity

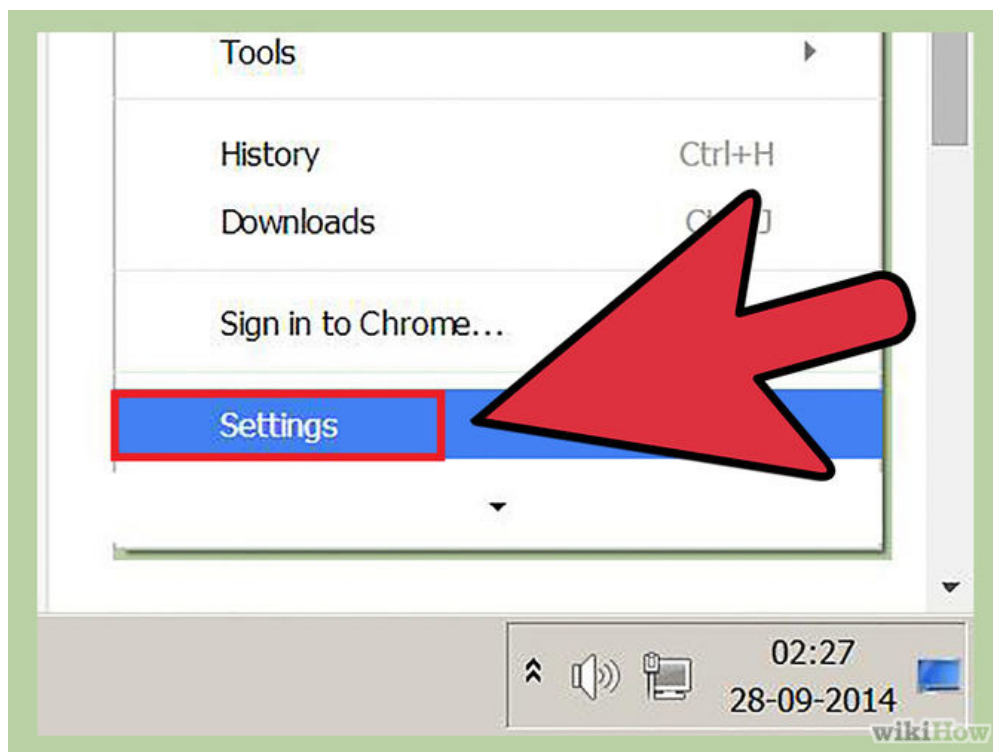
1. Find out whether the popular websites you visit daily are secure or not.
2. Can you find any banking site that does not use https://
3. Can you find some social networking site that does not use https://
4. Can you list down some important points that should be kept in mind before going for online shopping.

UNIT V: How to Clear Your Browser's Cache

1.6 CLEARING CACHE FOR BROWSERS

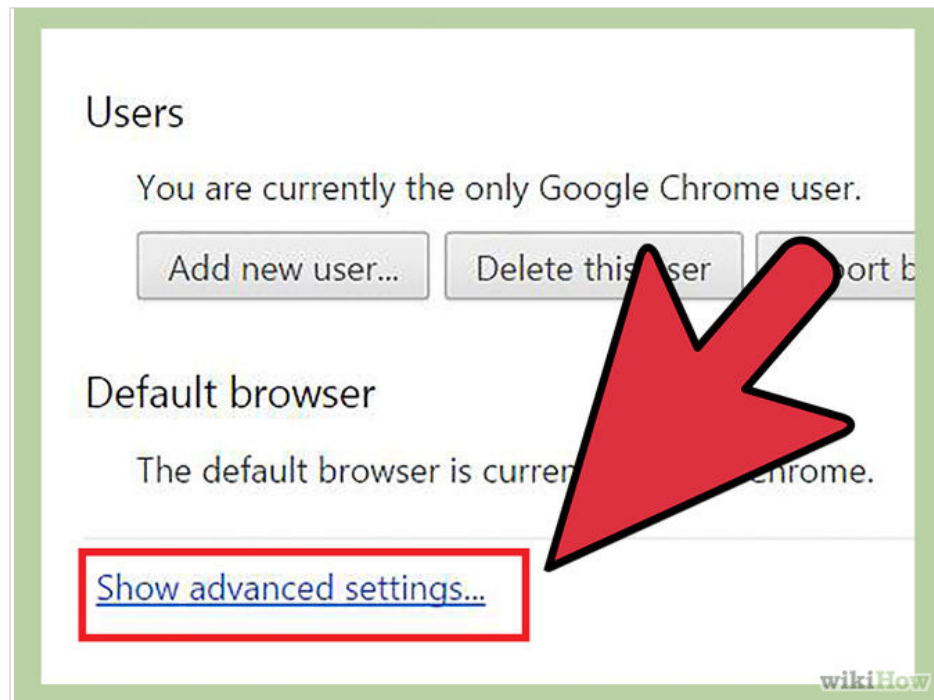
Your internet browser's cache stores certain information (snapshots) of webpages you visit on your computer or mobile device so that they'll load more quickly upon future visits and while navigating through websites that use the same images on multiple pages so that you do not download the same image multiple times¹⁰. Occasionally, however your cache can prevent you from seeing updated content, or cause functional problems when stored content conflicts with live content. You can fix many browser problems simply by clearing your cache. This article contains instructions with screenshots on how to clear the cache for all major browsers.

1.6.1 Clearing cache for Chrome Browsers above version 10

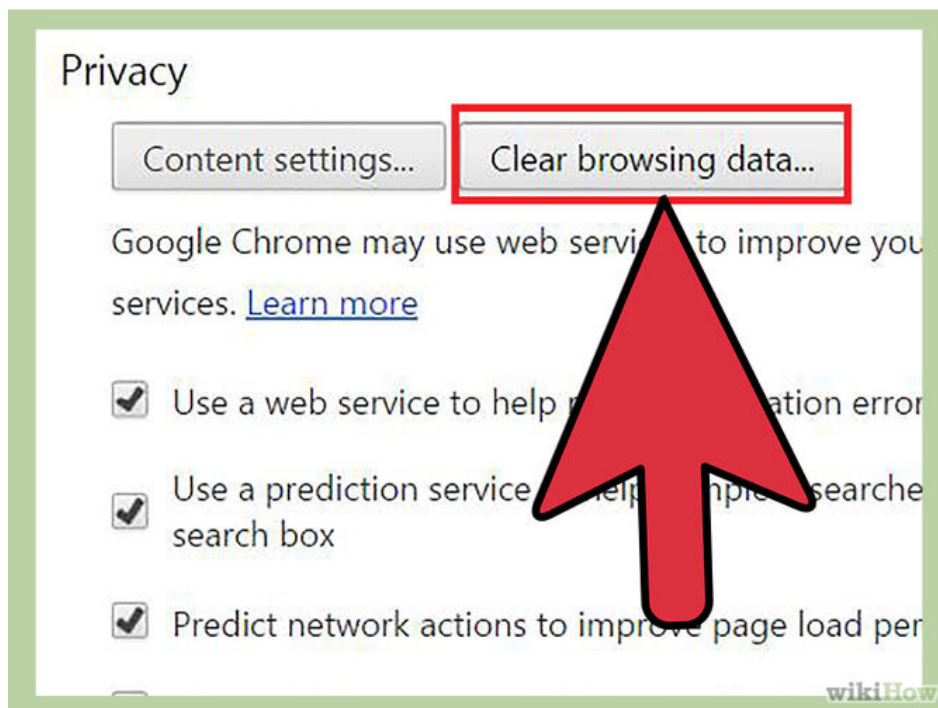


Step 1: Open the settings on Chrome. Click the menu icon in the upper right corner of the browser to the right. Click settings on the bottom of the menu.

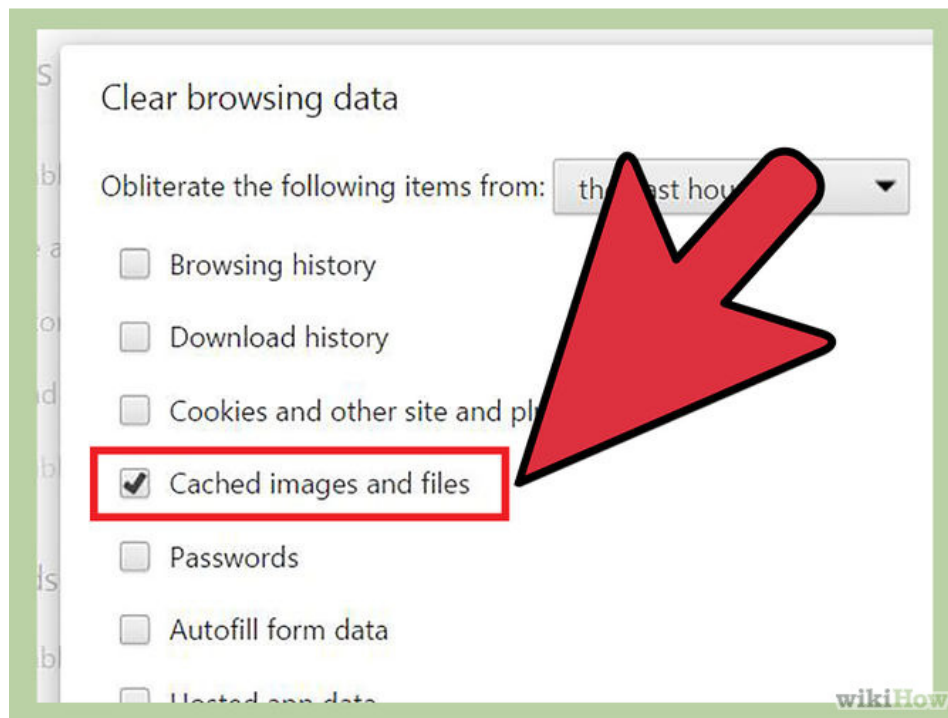
¹⁰ <http://www.wikihow.com/Clear-Your-Browser%27s-Cache>



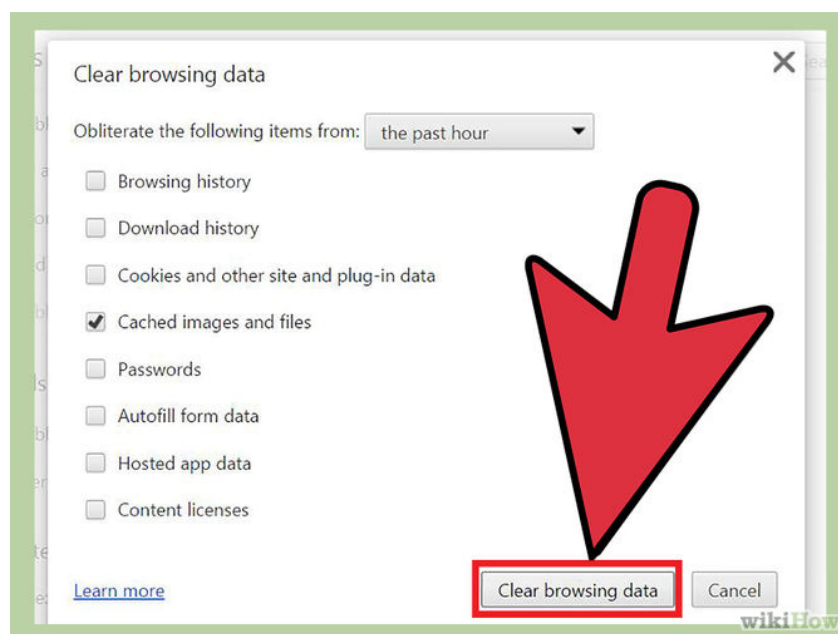
Step 2: From settings, click "Show advanced settings. It's located at the very bottom of the settings section.



Step 3: Scroll to the privacy section and click "Clear browsing data.

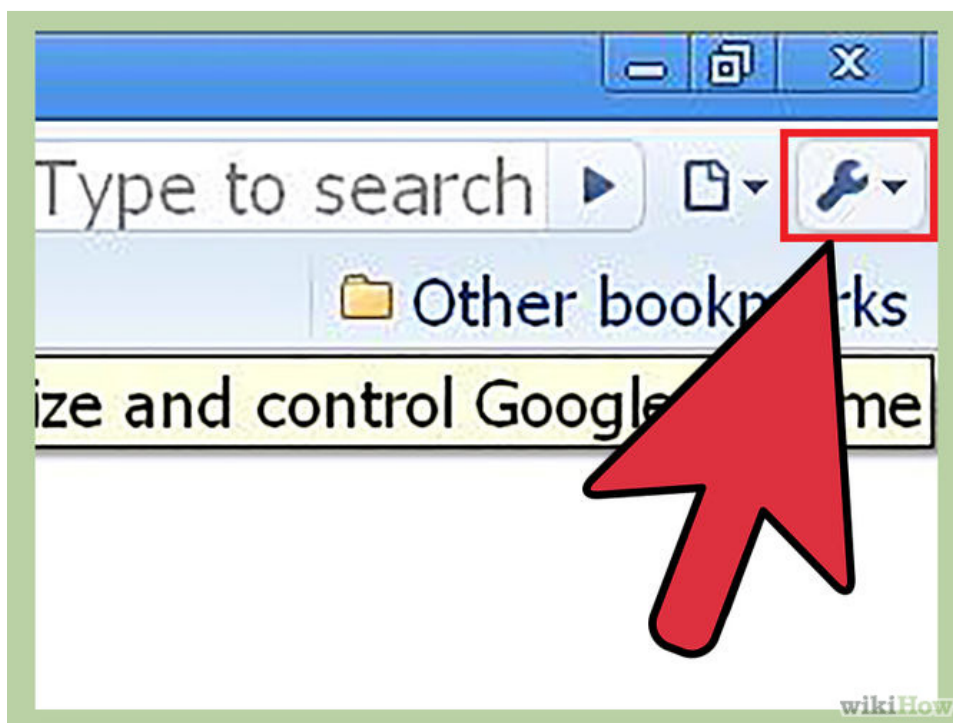


Step 4: Select "Cached images and files". Uncheck all other options to avoid deleting browser history, cookies and other things you may wish to retain. Change "Obliterate the following items from" to "the beginning of time".

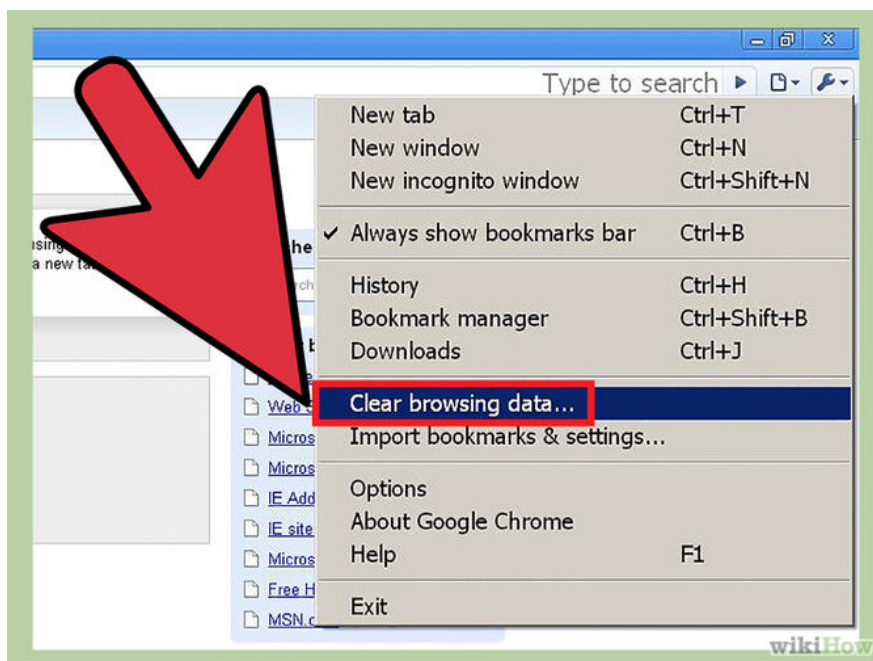


Step 5: Press "Clear browsing data". You are done!

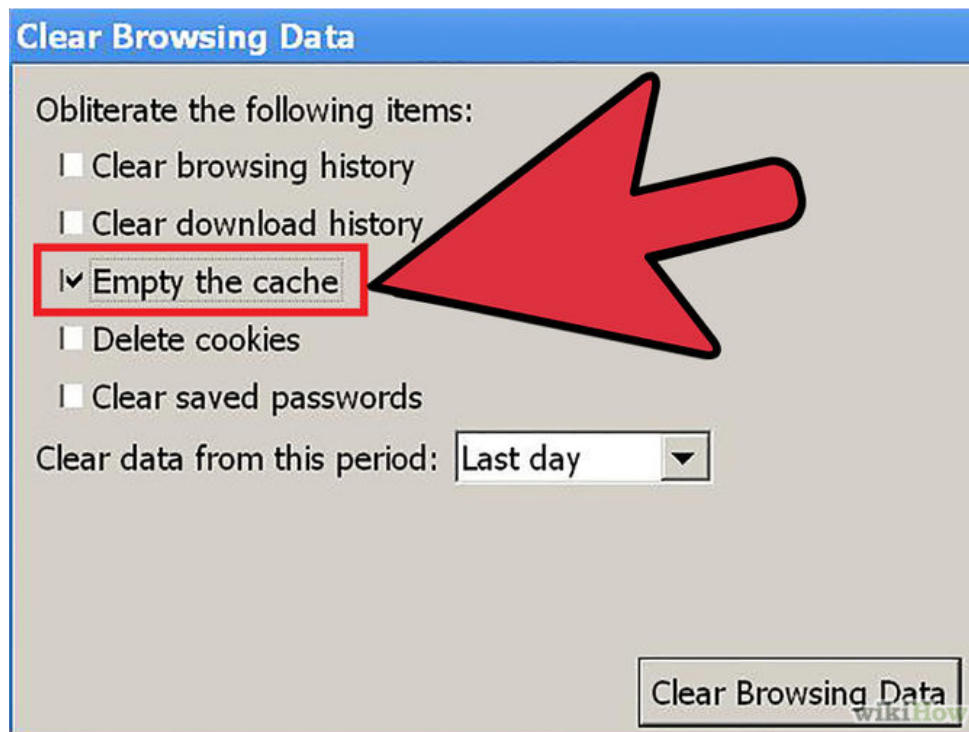
1.6.2 Clearing cache for Chrome Browsers from version 1 to 9



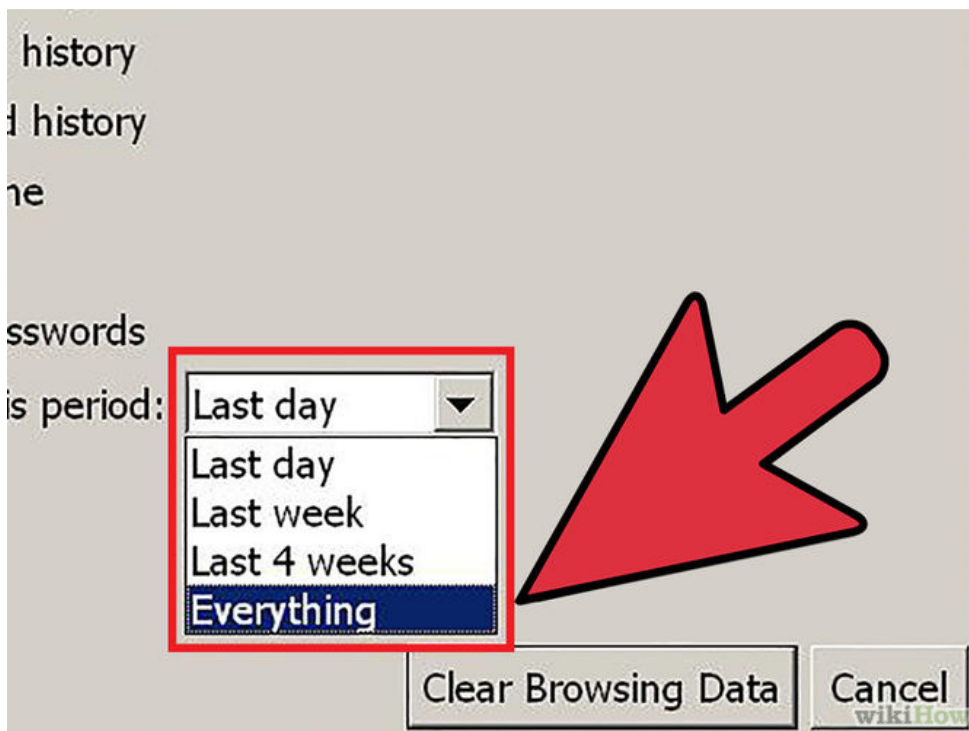
Step 1: Once your browser is open, select the Tools menu (the wrench in the upper-right corner) and select Options (Preferences on Mac).



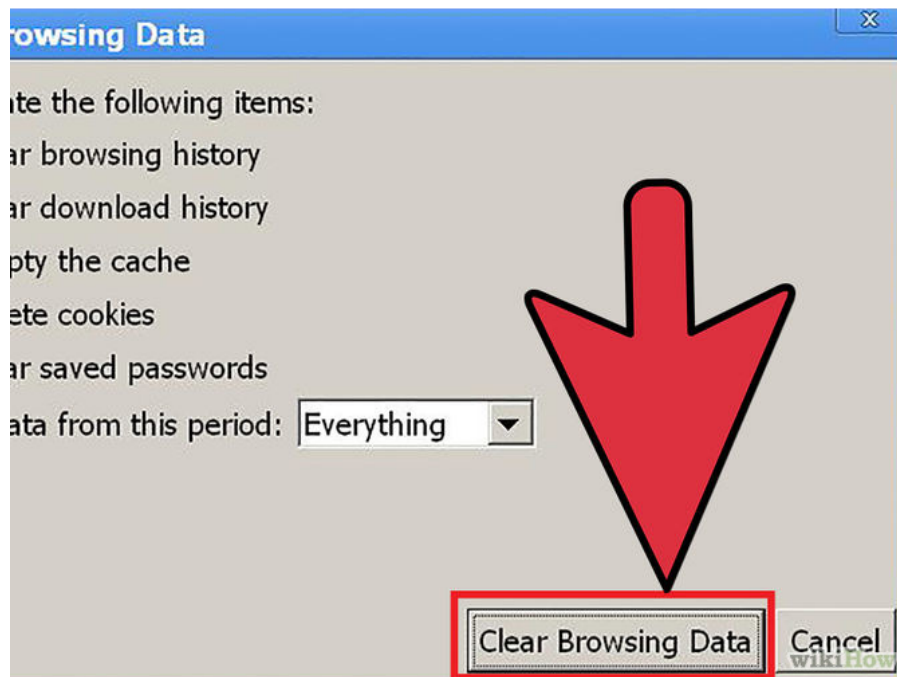
Step 2: On the Under the Hood tab, click the **Clear Browsing data** button.



Step 3: Select the Empty the cache check-box.



Step 4: You can also choose the period of time you wish to delete cached information using the Clear data from this period dropdown menu.

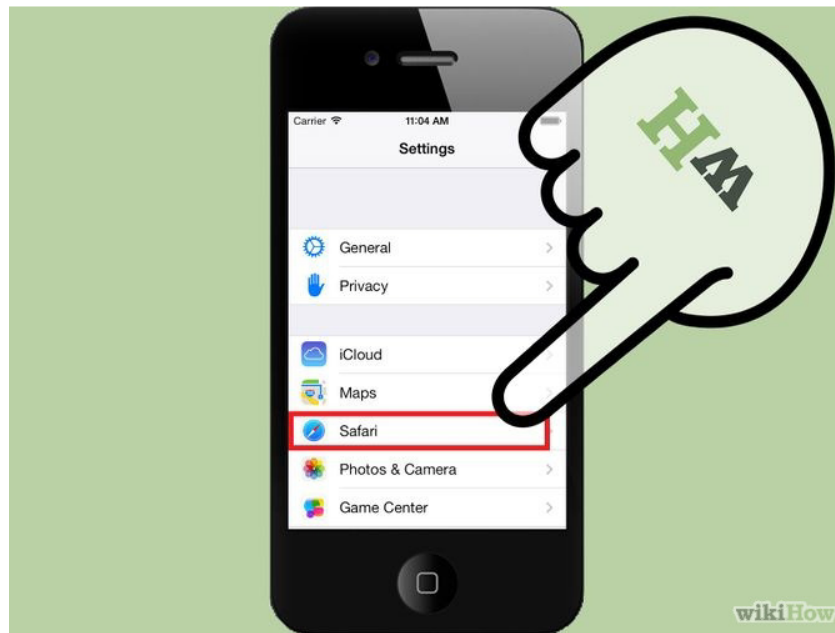


Step 5: Click the Clear Browsing Data button.

1.6.3 Clearing cache for Safari for iOS, iPhone and iPad



Step 1: Click on Settings from the home page.

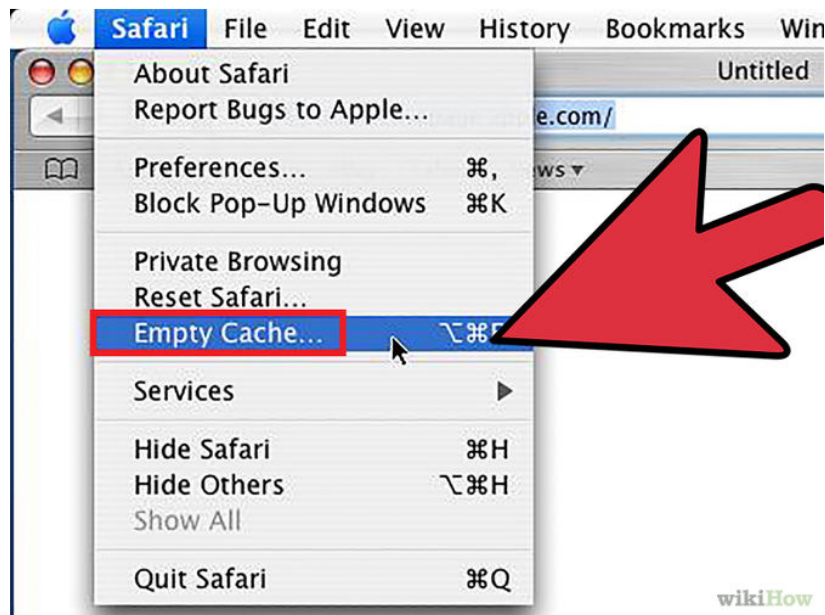


Step 2: Scroll down until you see "Safari." Click on it to bring up the option page.

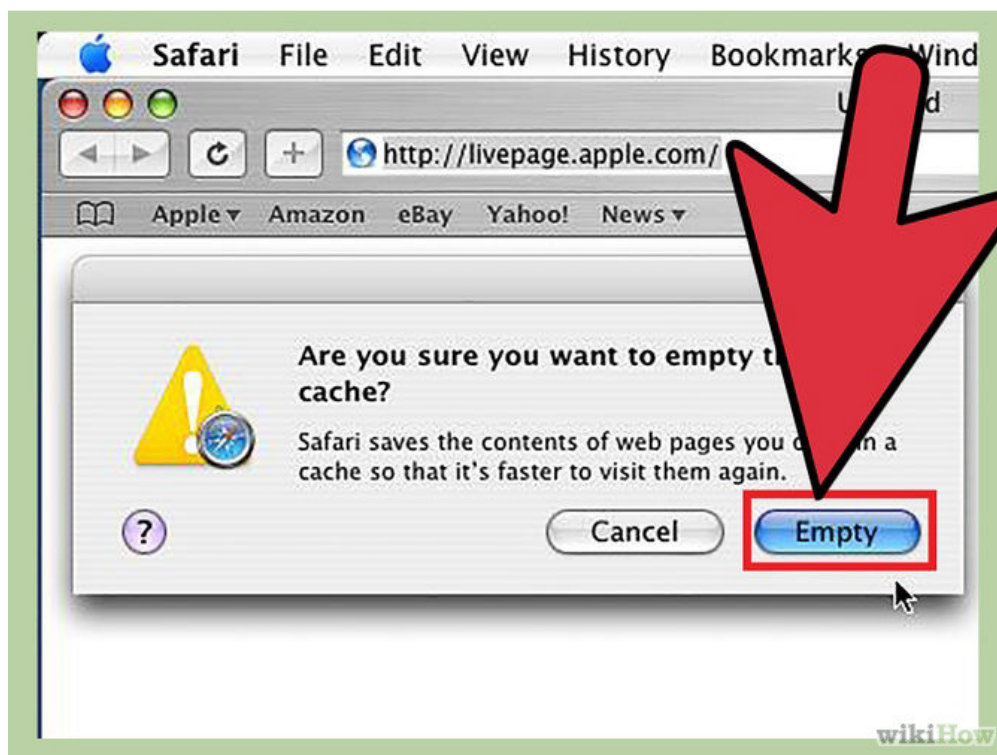


Step 3: Click "Clear Cookies and Data". A popup box will appear. Click "Clear Cookies and Data" again to confirm your choice.

1.6.4 Clearing cache for Safari for Mac OS x



Step 1: Once your browser is open, click the Safari menu and select Empty Cache.

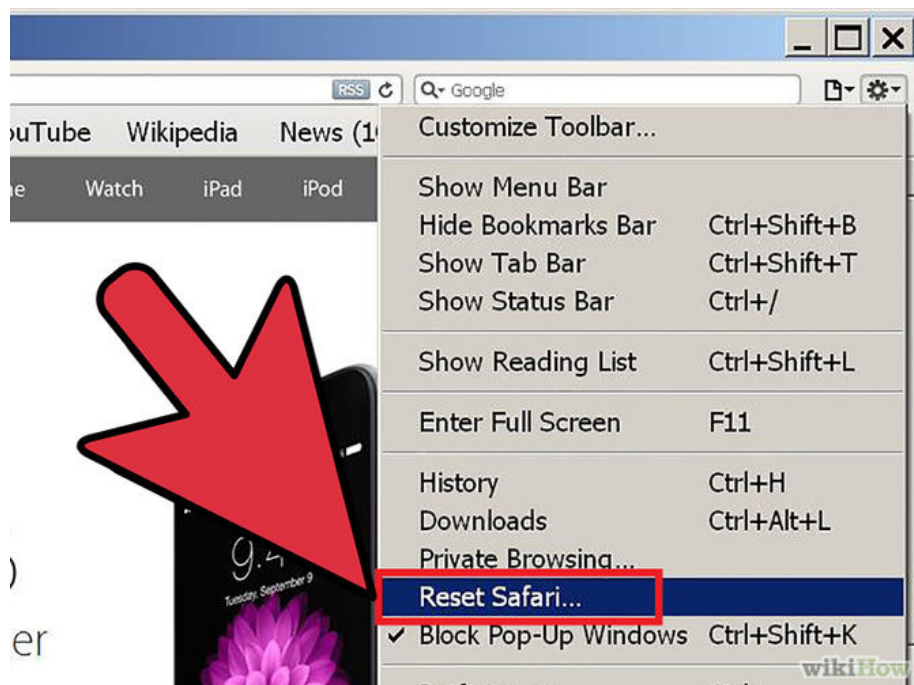


Step 2: Click Empty.

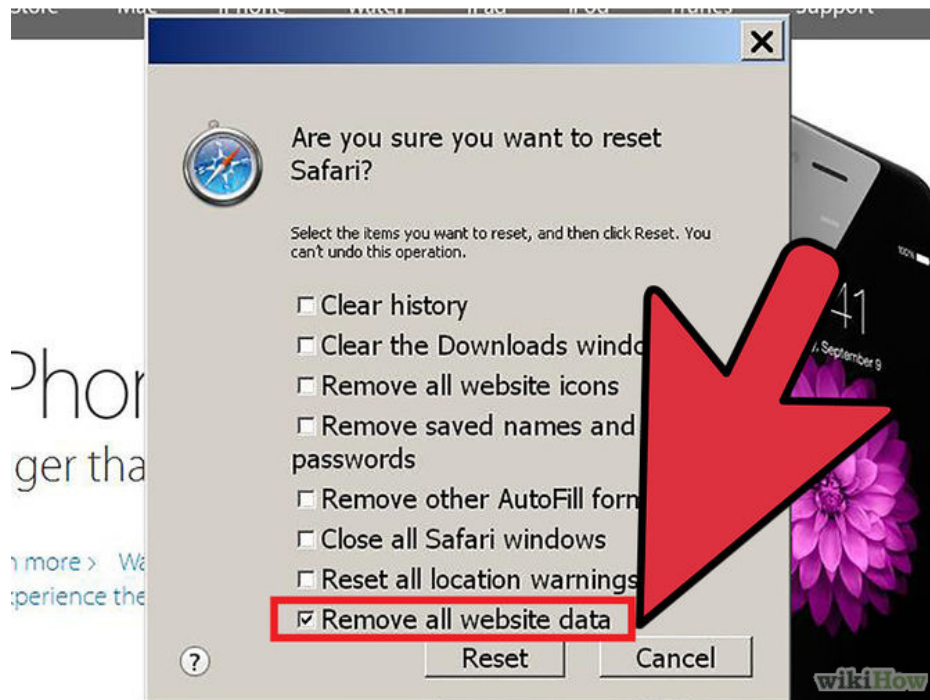
1.6.5 Clearing cache for Safari for windows



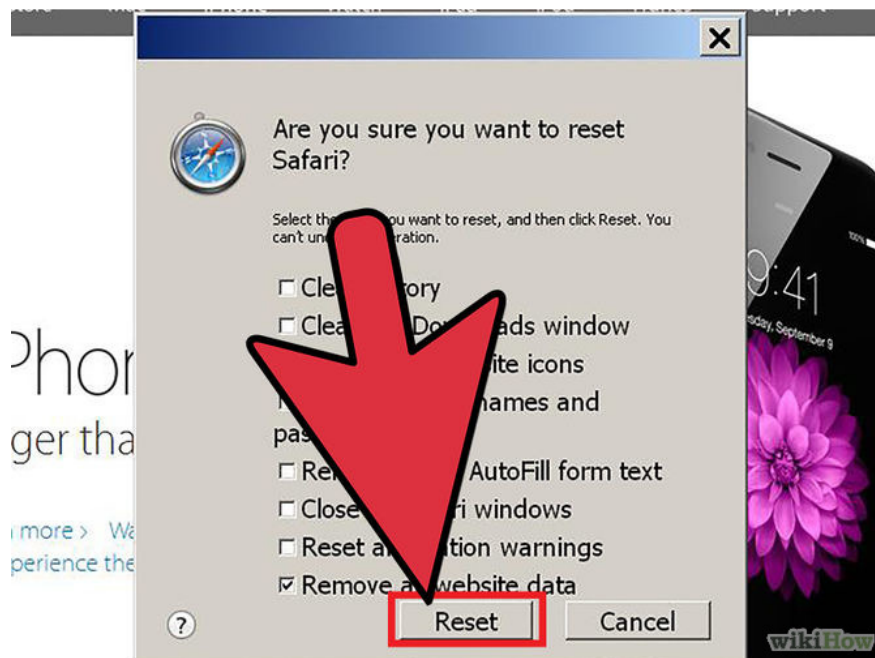
Step 1: Once your browser is open, click the gear icon on the top right.



Step 2: Select "Reset Safari..." This will prompt a screen to open.

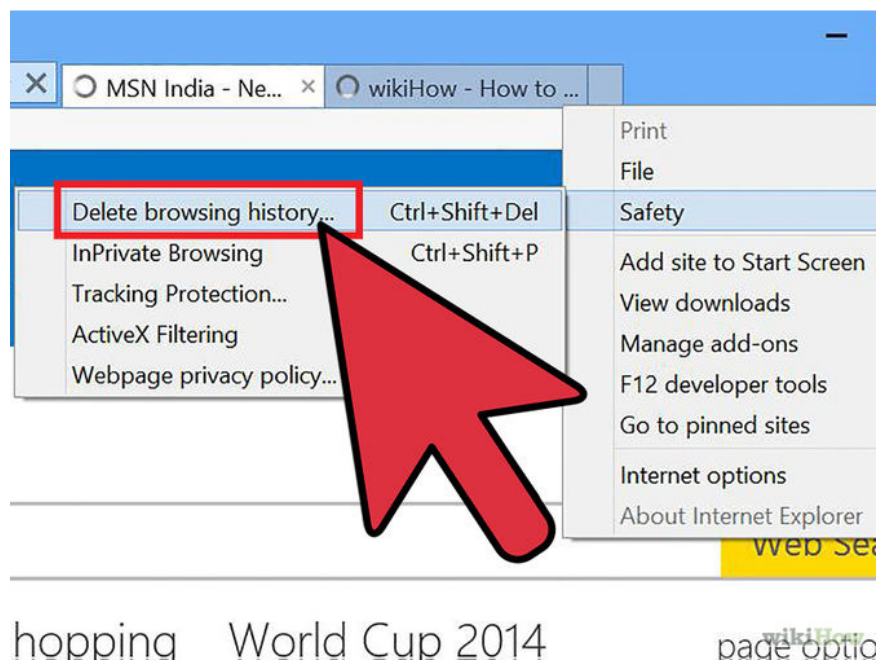


Step 3: Select "**Remove all website data**" at the very bottom of the prompt. Check or uncheck any other categories you want reset.



Step 4: Click "Reset".

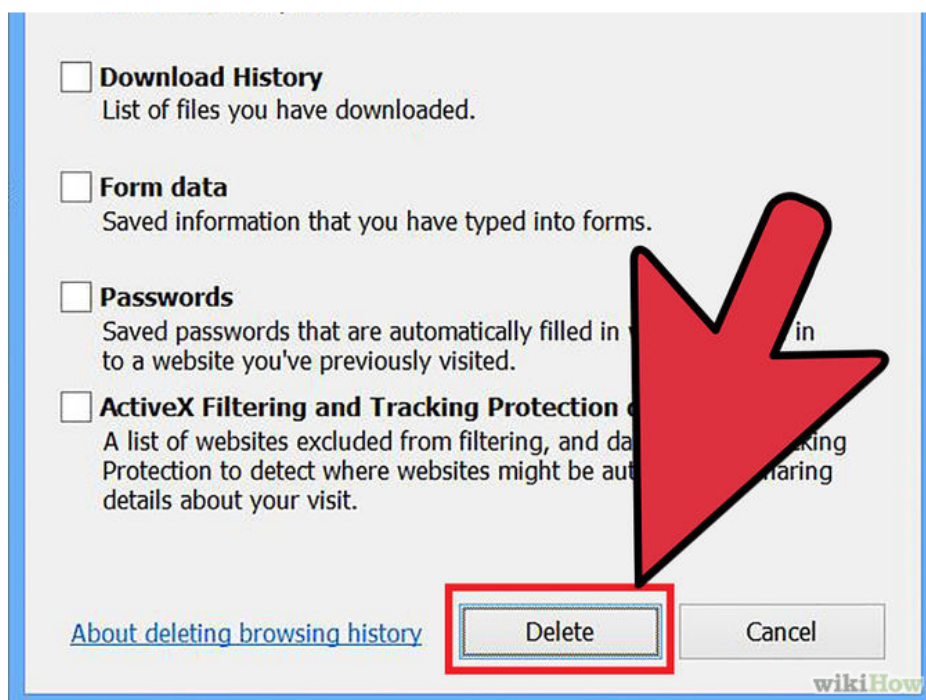
1.6.6 Clearing cache for Internet explorer 9, 10 and 11



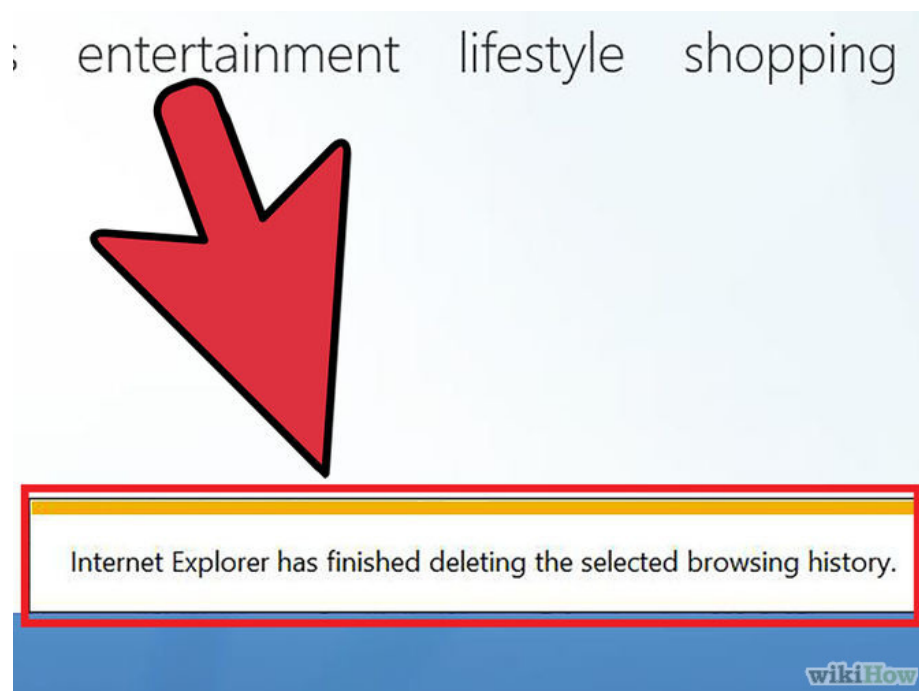
Step 1: Once your browser is open, click the gear icon at the top right to open the **Settings** menu. Then, select **Safety** and **Delete Browsing History**.



Step 2: Select Temporary Internet Files. You will also need to uncheck all of the other boxes, especially Preserve Favorites website data. This option makes the window also delete objects from websites in your Favorites folder, which is necessary to completely clear your cache.



Step 3: Click the Delete button near the bottom of the window to perform the operations (i.e. clear your cache by deleting temporary files).

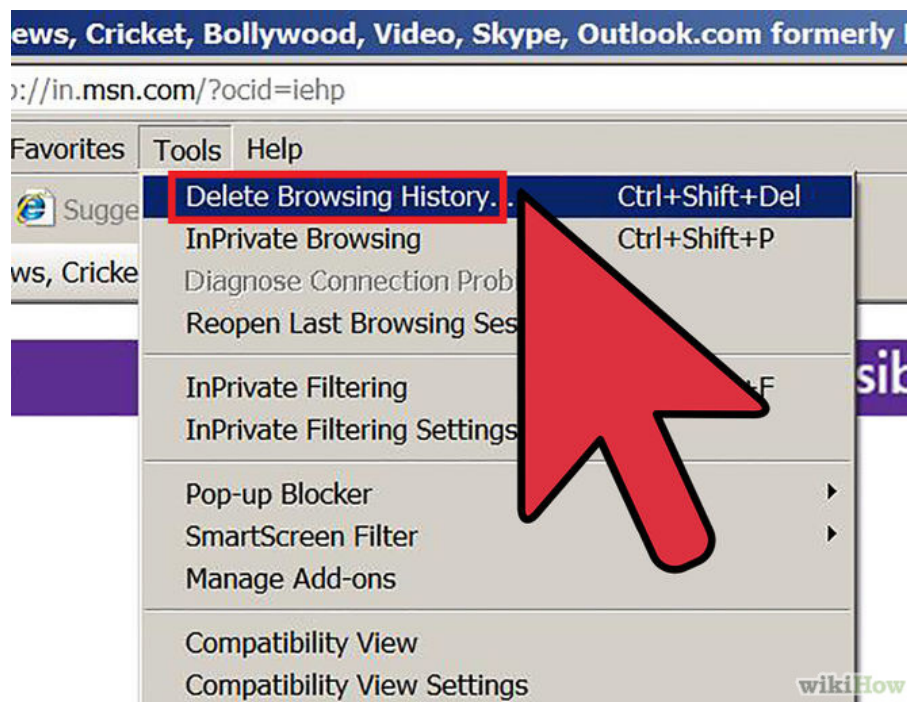


Step 4: Your computer will work for a moment, and then the process will be complete. You've successfully cleared Internet Explorer 9's Cache!

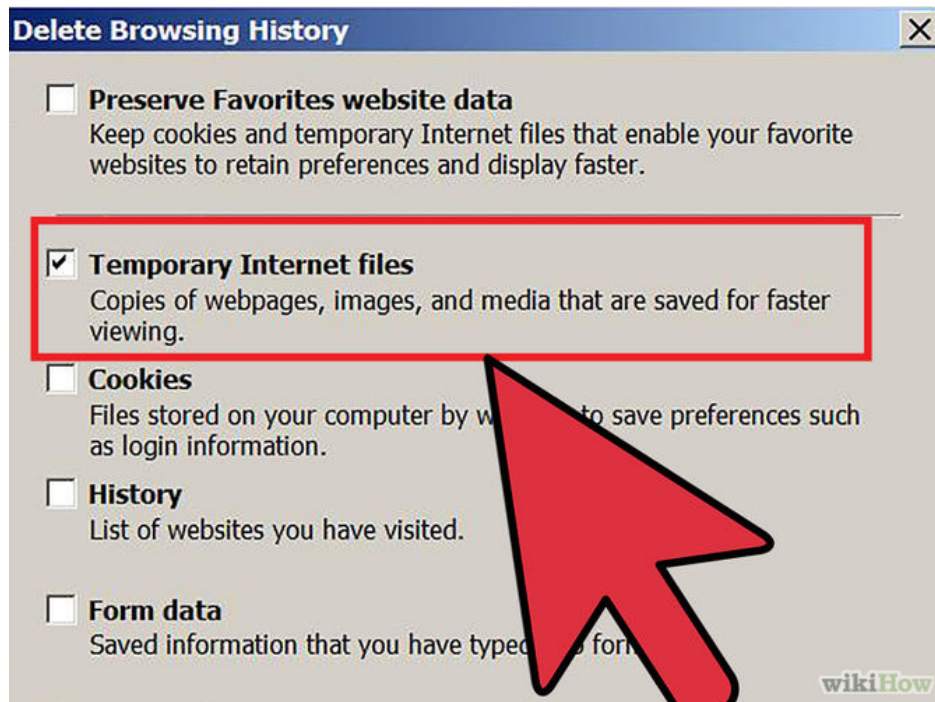
1.6.7 Clearing cache for Internet explorer 8



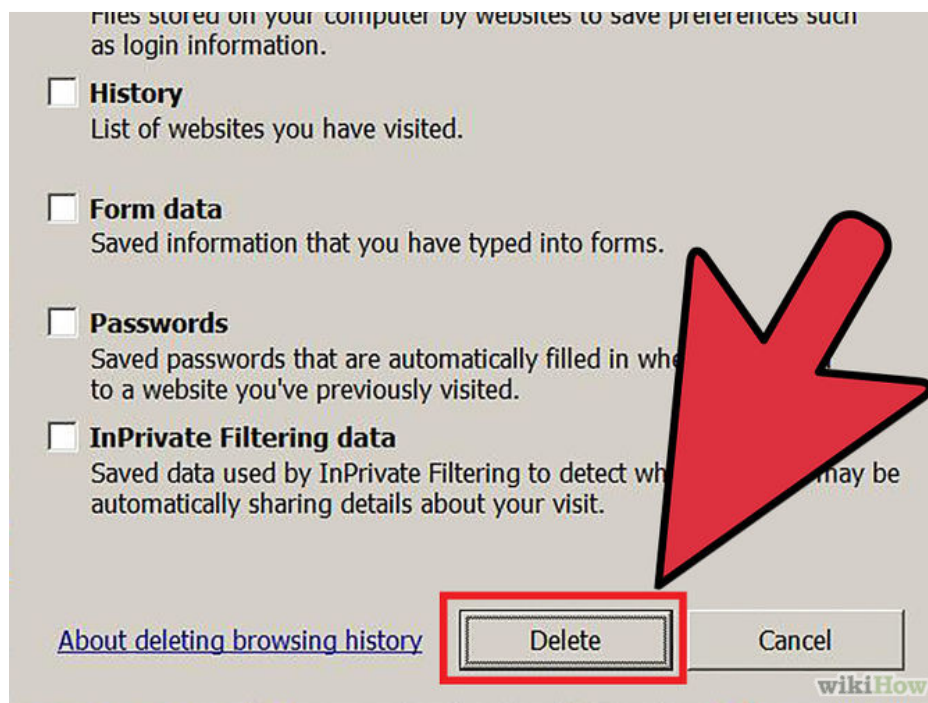
Step 1: Once your browser is open, click the **Tools** menu.



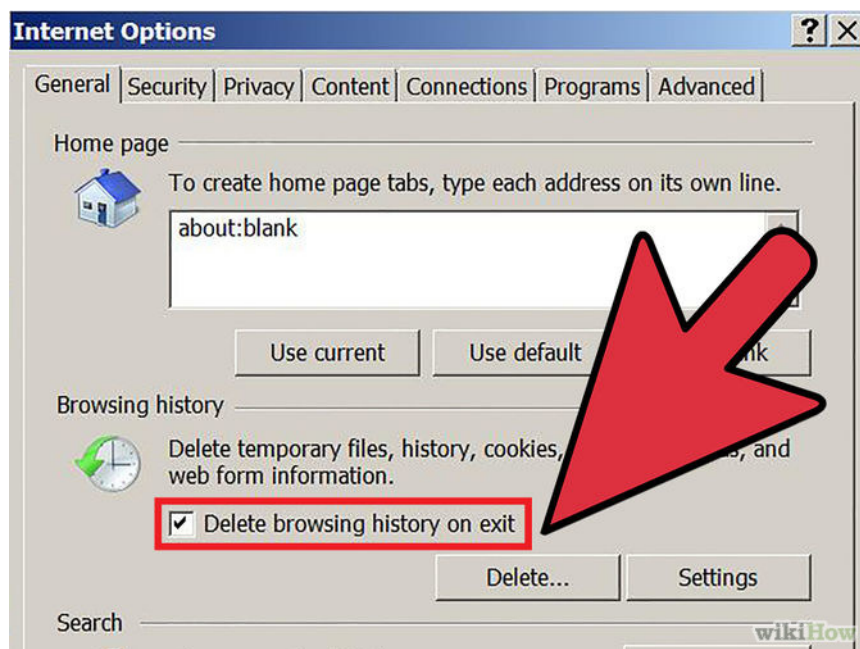
Step 2: Click on **Delete Browsing History**.



Step 3: Select **Temporary Internet Files**.



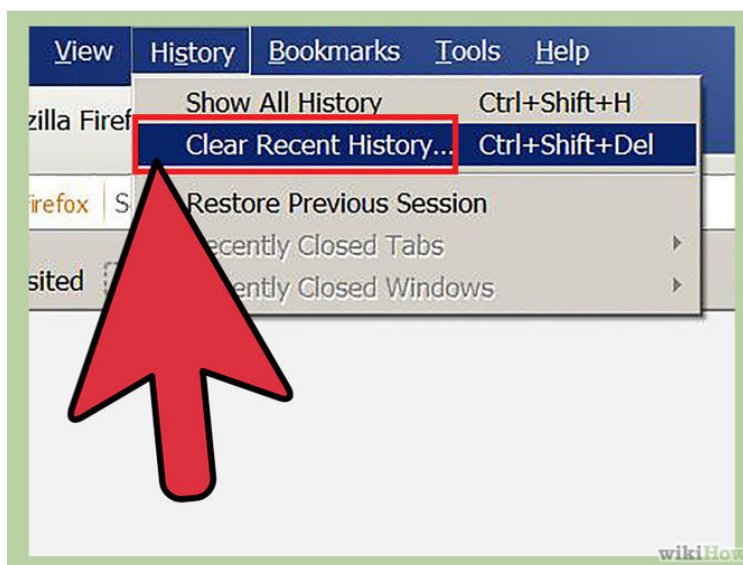
Step 4: Click the **Delete** button near the bottom of the window to delete your temporary files (i.e. clear your cache).



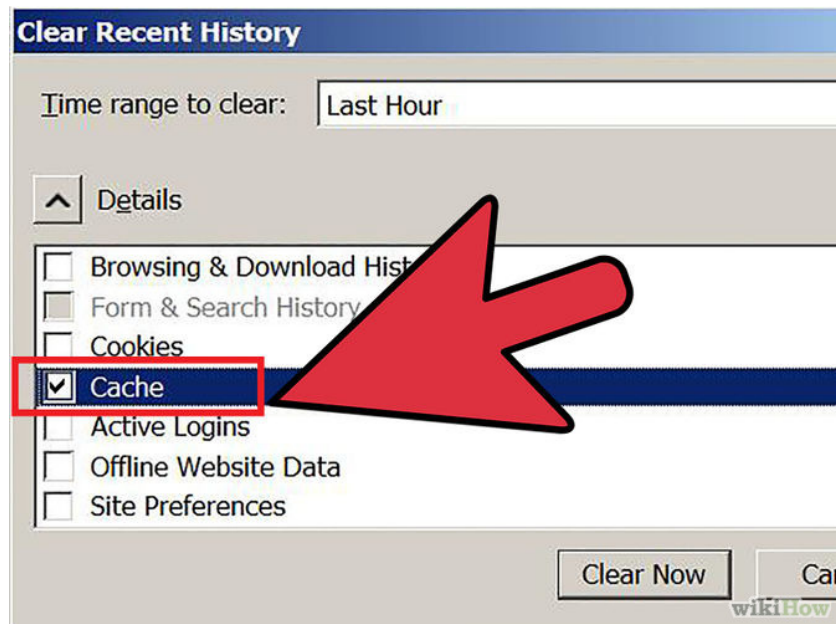
Step 5: Set your cache to delete every time you close Internet Explorer. If you want the browser to automatically clear the cache whenever you close it, close the 'Delete Browsing History' window, select '**Internet Options**' from the Tools menu, and check the '**Delete Browsing history on exit**' checkbox.

Note: IE8 has a "feature" which retains some cookies even after you clear your cache if you do not UNCHECK the "Preserve Favorites Website Data." If you truly need to clear your cache, you will want to uncheck this!

1.6.8 Clearing cache for Firefox



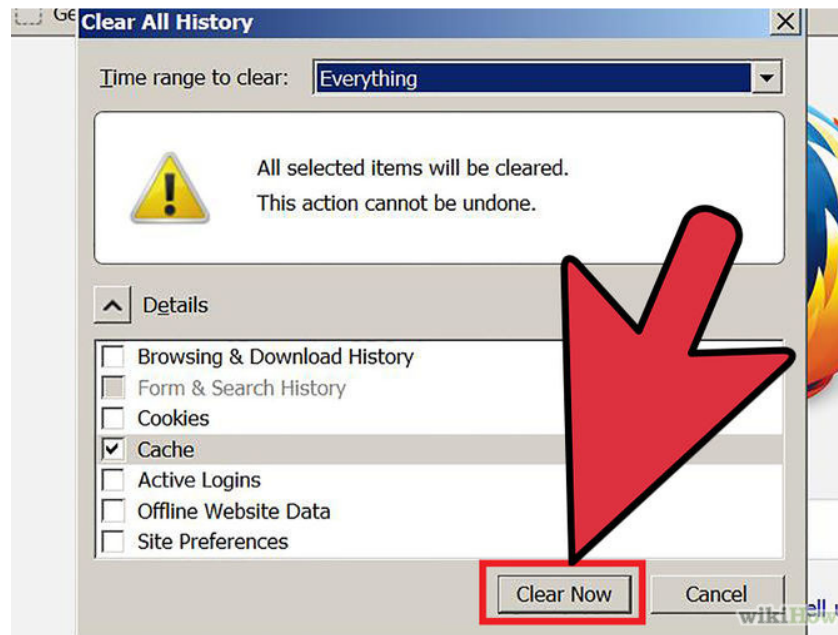
Step 1: On a PC, click the "Firefox" menu in the top left corner. Next, select the right arrow next to "**History >**", and click "**Clear Recent History**".



Step 2: Make sure "**Details**" is expanded, then select "**Cache**" from the list. Uncheck everything else.

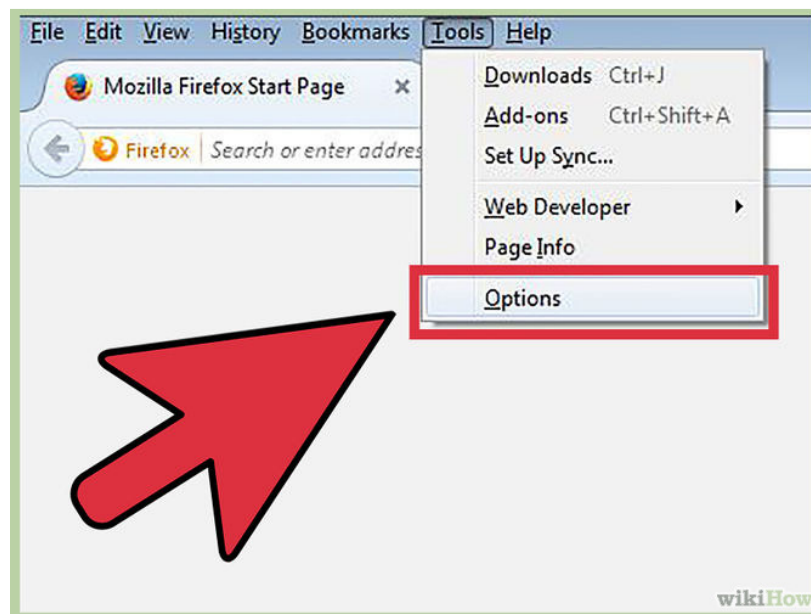


Step 3: In the "**Time Range to Clear**" drop down, select "**Everything**".

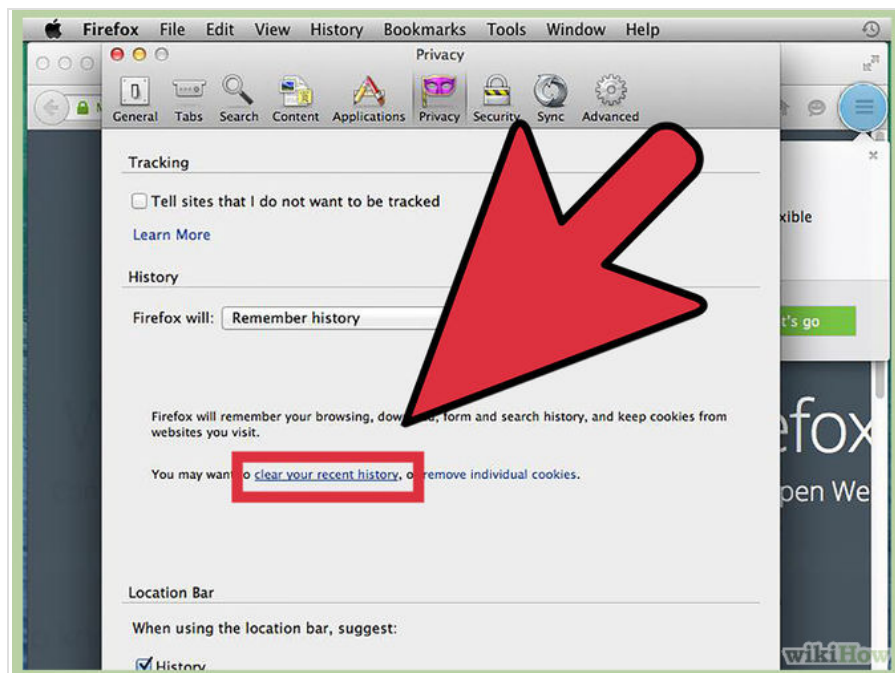


Step 4: Select "Clear Now". Your computer will work for a moment, and the process will be complete. You've successfully cleared Firefox's Cache!

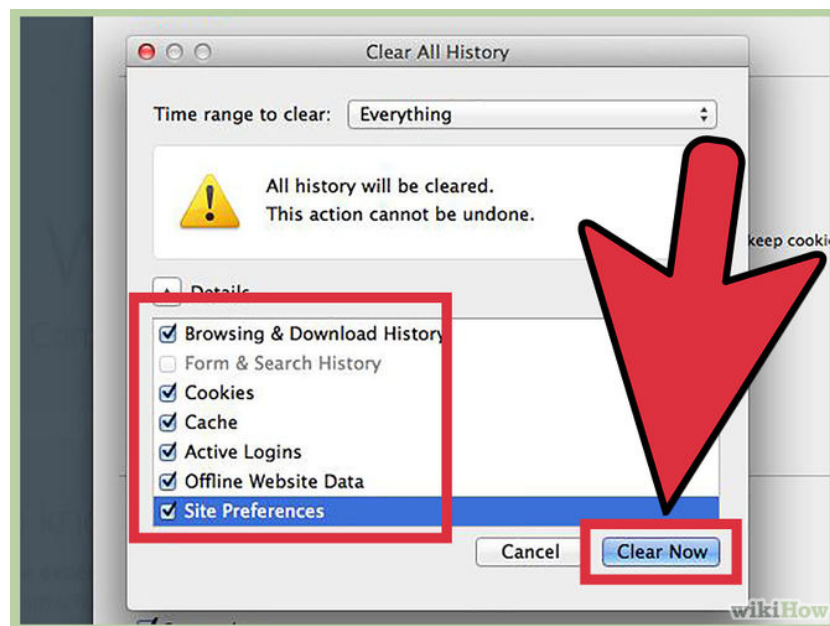
1.6.9 Clearing cache for firefox 33



Step 1: Click the Menu button ("hamburger button" - the one with three horizontal lines) and then choose Options.

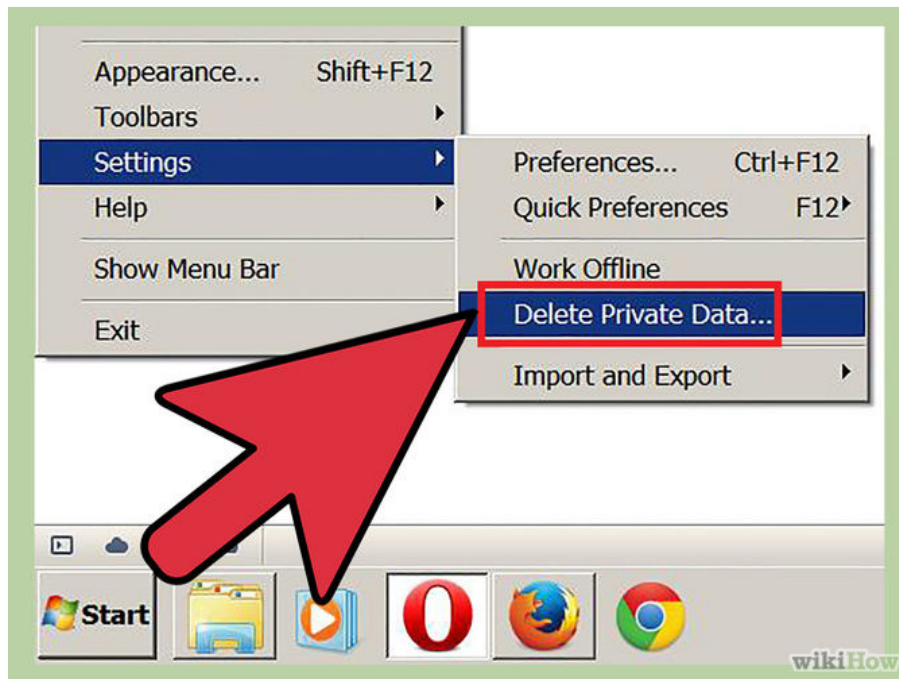


Step 2: Firefox for Mac: On a Mac, choose Preferences from the Firefox menu and then continue as instructed below. With the Options window now open, click the Privacy tab. In the History area, click the clear your recent history link.

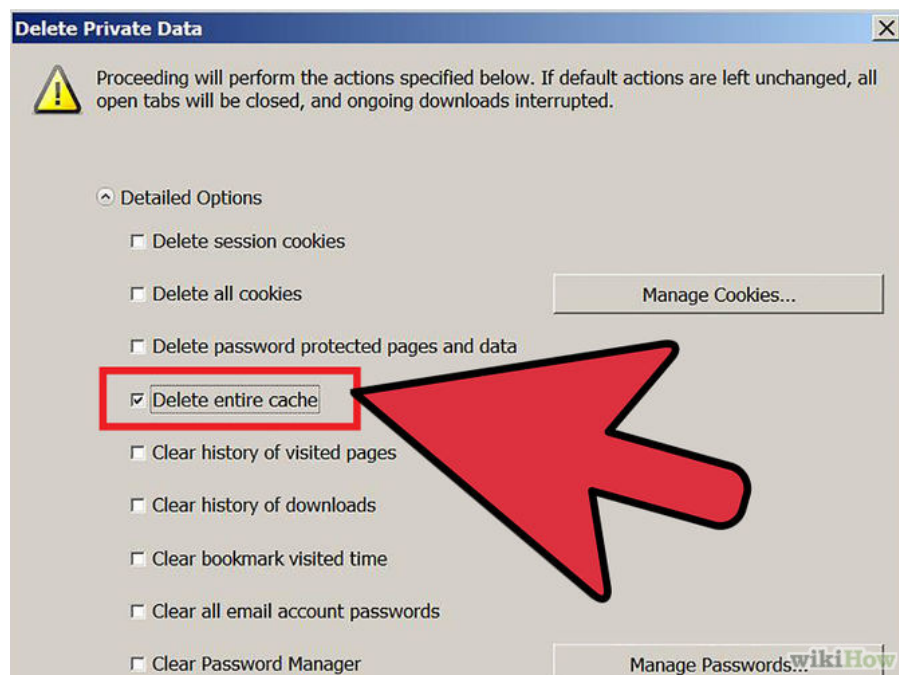


Step 3: If you wish to clear other kinds of stored data, feel free to check the appropriate boxes. They will be cleared with the cache in the next step.

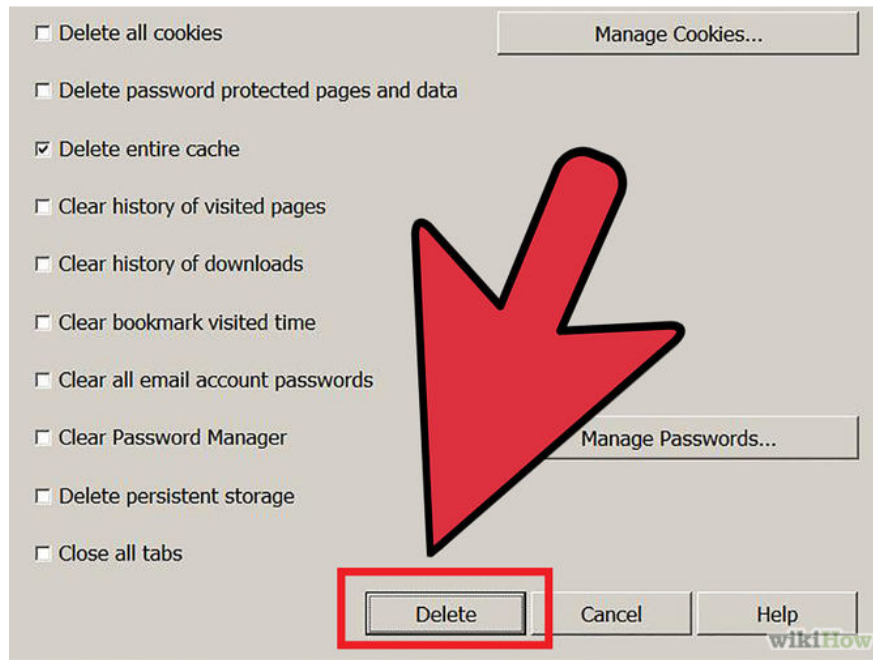
1.6.10 Clearing cache for opera



Step 1: Once your browser is open, select the "Settings" menu and click "Delete private data".

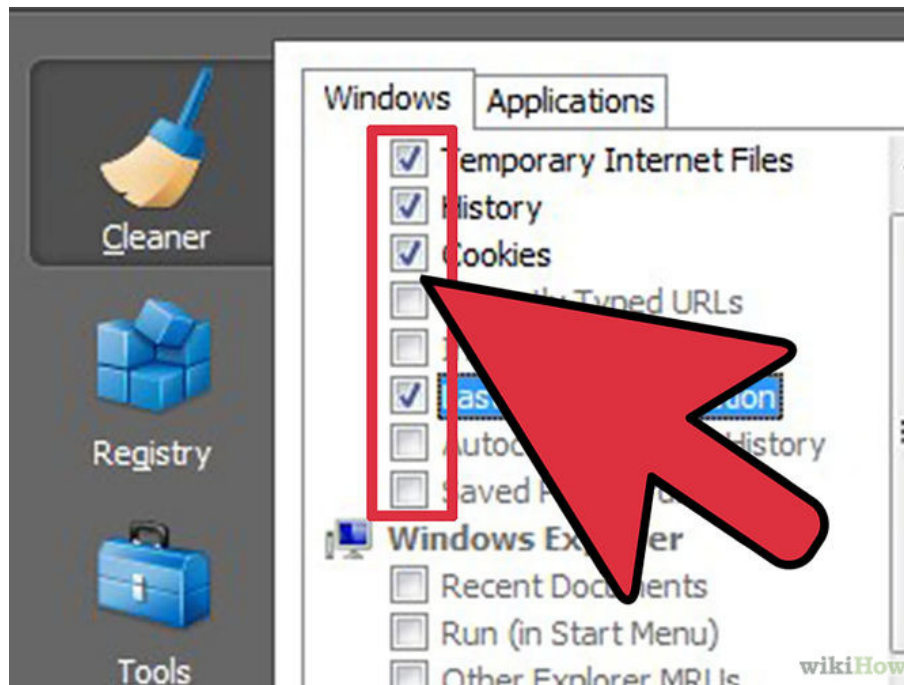


Step 2: Make sure the "Delete entire cache" box is checked. Make sure any unwanted categories are left **unchecked**.



Step 3: Press “Delete”.

1.6.11 Clearing cache for Ccleaner



Ccleaner- This is a computer maintenance tool that lets you scan and delete browser cache and cookies. Launch it, go to Cleaner tab and make sure to check the Temporary internet files for the browser you have.

Activity

1. Perform the cache clearing operation on your system browser.
2. Perform the cache clearing operation on the browser of your smartphone.
3. Install Ccleaner in your system and use it to perform cache clearing operation.

UNIT VI: Securing Wi-Fi network

1.7 WIRELESS SECURITY – BEST PRACTICES

This section is about different kind of Best Practices that should be followed when using Wireless LAN.

1.7.1 What is Wireless LAN?

The Wireless LAN or WLAN is becoming a popular way to connect devices such as computers these days. In offices and homes, WLAN has become an alternative way of communication compared to wired LAN. The convenience to connect different devices is both cost effective and easily maintainable.

The Wikipedia says: “Wireless LANs have become popular in the home due to ease of installation, and the increasing to offer wireless access to their customers; often for free.”

The other factors why WLANs are becoming more acceptable are:

1. No need to be connected physically with each other through any medium such as cables. You can roam around freely in office premises, home or around.
2. WLANs are cost effective. Cabling all the way in the offices, hotels etc are not needed. So it's cheap and provide same quality of service.
3. Unreachable spots where a cable is hardly accessible, WLAN signals can reach out such as big installations like airports. Also surfing outdoors is also convenient. Just install the device called Access Points (AP) and you are done.
4. Less interruption and easy trouble shooting in case of failures as compared to cabled networks.
5. More secure as most of APs support best encryption methods which protect them from sniffing and other attacks.

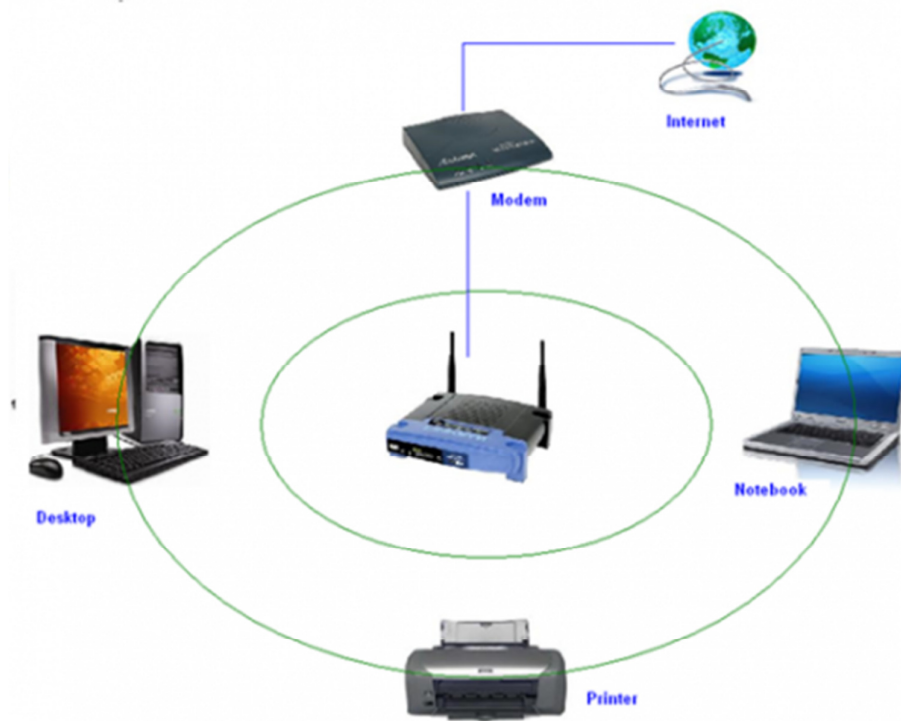


Figure 7: A typical Wireless network

1.7.2 Major issues with WLAN

Having said that, WLAN are also as prone to various attacks as their counterpart wired LANs are. Actually WLANs are easier to hack as compared to wired LANs, if not properly configured, due to its easy accessibility around the installation. No need to be in contact of physical wires to hack, can be done from anywhere. Its convenience can turn into serious risk to the organization if not configured properly. Major attacks include such as, Sniffing, Key cracking, DoS (Denial of Service), Deauthentication attacks, War driving etc. This chapter is not focused on attacks, we shall mainly concentrate on best practices- how to install and use WLAN securely which can thwart a number of above mentioned attacks.

1.7.2.1 Secure WLAN

Wireless Security mainly depends on these 3 factors:

- How much is your wireless network secured in terms of encryption being used.
- Monitoring for suspicious and unusual activities.
- User awareness and education.

These are the combination of various approaches ranging from corporate to home networks. These are also for users how to remain safe while surfing.

1.7.2.2. Wi-Fi at home

Using a Wi-Fi at home is not a luxury anymore it has become a necessity. However, when the question of security comes into the scene, the first thought that would arise in my mind is how you can protect something which you cannot see, neither can you feel it? Protecting a home wireless network is altogether a different side of the coin as compared to wired networks. Most of wireless network device vendor's and Internet Service provider do not provide any security settings by default and leave the customer to fend for herself. So make sure, your network is secured from being maliciously used.

There is no silver bullet that will protect your wireless network infrastructure. These are, however, some countermeasures listed below that should be used in conjunction with each other to secure your wireless network to the highest level:

1. Use most secure possible encryption: The first and most necessary step- use industry standard encryptions. The old (however generally used) WEP-Wired Equivalent Privacy, has been known to be broken. Even you use complex passwords it can be broken and decrypted within minutes or hours. WEP uses 40 bit or 128 bits RC4 ciphers to encrypt the channel. Instead use secure protocols such as WPA 2 – Wi-Fi Protected Access- 2, which uses strong 128 bits AES ciphers and is typically considered more robust encryption strategy available.

Attacks mitigated: WEP Key cracking, Sniffing, Capturing/Eavesdropping

2. Use Firewall: All the wireless routers come with built-in firewalls. Enable them with all the security features. You should block any anonymous ping requests and place restrictions on website browsing, if required. Define additional security policies and apply them.

Attacks mitigated: Fingerprinting, System compromise

3. Have a monitoring system in place: There's a saying- prevention is better than a cure. If you are able to detect some suspicious activities before it penetrates your network, you can block them or take precautionary measures. Deploy WIPS/WIDS for monitoring suspicious activities.

Attacks mitigated: Scanning, DoS

4. Don't use default credentials: Every wireless router comes with a set of default username/password. Sometimes, people don't change them and keep using them for long time. Username and passwords are used by computers or other devices to connect to wireless router. If any hacker is able to guess them, he can connect to your network easily. Studies

show that majority of users use the same combination of username/passwords as set by manufacturers. Some default username combinations are: admin/admin, admin/password or admin/ “ “.

Attacks mitigated: Unauthorized access, War driving

5. Disable Auto-connect feature: Some devices or the computers/laptops have ‘Let this tool manage your wireless networks’ or ‘Connect automatically to available network’. Such users having this auto-connect feature enabled are prone to Phishing attack or Rogue AP attack. Attackers keep their APs alive and kicking for such kind of unsuspecting users. They also use luring names as ‘HotSpot’, ‘SecureConnect’, ‘GovtNetworks’ etc. The user will never suspect them and keep surfing the wireless network happily. Also if you have not changed the default password of your router, the attacker will try to use this feature on their machine and automatically connect using the easily guessable default passwords.

Attacks mitigated: Phishing, Sniffing, Rouge AP association

6. Don’t use public Wi-Fi spots to surf sensitive websites: Free and open wireless networks available on airports, cafes, railway stations are not very secure by nature. They do not use any encryption to secure the channel between your laptop to the router. So any information which is not by default going on HTTPS from your laptop/smart phone is susceptible to sniffing and even more your session could be hijacked because the unencrypted channel may leak the active session ID used by your website. Recently to demonstrate these types of attacks one researcher developed a tool Firesheep [<http://codebutler.github.com/firesheep/>]. All the attacker needs to do is to just install this tool in Firefox and start sniffing the communications on a public unencrypted Wi-Fi. Some applications like Facebook encrypts the login page [HTTPS] but internal pages are served on unencrypted [HTTP] channel so your session ID can be leaked.

Attacks mitigated: Sniffing, Session Hijacking

7. Change the default SSID: Although this will not prevent hackers breaking into a network, using a default SSID acts as an indication that the user is careless. So he may be an obvious target to explore further to see if he still uses the default passwords as well?

Attacks mitigated: War driving

8. Restrict access by assigning static IP addresses and MAC filtering: Disable automatic IP assigning feature and use private static IPs to the legitimate devices you want to connect. This will help you in blocking unwanted devices from being connected to your network. Also, enable MAC filtering- router remembers MAC of each and every device connected to it and saves it as list. You can use this facility to restrict access. Only a set of trusted devices can be allowed to connect. However MAC spoofing is still possible but it raises an extra bar for your wireless network.

9. Turn off your router when not in use: Last but not least, a little obvious, but it will save your network from all the attacks for that time period.

1.7.2.3 Wi-Fi in a Corporate/Enterprise Network

Due to the nature of activity and criticality of information, it is very important that Corporate / Enterprise networks have a higher degree of security.

The following are good to have:

- Defining an adequate organization wide Information Security policy & procedures for wireless network
- SSID's should not be associated with the organization, AP vendor or any other related information which would be easy to guess or associate with the current organization
- Enable WPA2 Enterprise encryption with RADIUS authentication and use of EAP protocol like EAP-TTLS, TLS etc.
- Implementation of PKI infrastructure. CA signed certificates to authenticate the server to client and vice versa
- Filtering of clients based on unique identifier like MAC Address
- Isolated 'Guest' wireless network with no interface / connection to the corporate network
- Limiting the radius of Wi-Fi network by reducing the power output of the AP
- Allocating IP Address to the employee and guest machines only after successful authentication
- Periodically changing the keys & passwords
- Use of VPN while accessing corporate information from Public Wi-Fi network
- Client side utilities like DecaffeintID can help in detecting changes in ARP table and serve as common man's IDS to protect against attacks like 'hole196' and DoS.

- Implementation of Wireless IDS. Wireless IDS is a new concept. The key features of Wireless IDS are:

- Prevention against Rogue AP's
- Detection & prevention against DoS attacks
- Assistance in locating the approximate physical location of the attacker
- Assistance in enforcing the Organization's Information Security policy on wireless networks
- Detection of use of scanning tools like Kismet & NetStumbler

ACTIVITY

1. What are the precautions one should take using a wi-fi network at public place?
2. How to secure home network?
3. How to secure enterprise network?
4. Find more about the terms over internet:
 - IDS
 - DOS
 - Kismet
 - NetStumbler

RECOMENDED VIDEOS

https://www.youtube.com/watch?v=_WHynHcXm7c

https://www.youtube.com/watch?v=Jmszt__J204

<https://www.youtube.com/watch?v=aktovPyT0iM>

https://www.youtube.com/watch?v=CStMHLQWa_8

<https://www.youtube.com/watch?v=a9q-tDRCTtc>

<https://www.youtube.com/watch?v=xex1h93fnl8>

<https://www.youtube.com/watch?v=a9q-tDRCTtc>

UNIT VII: Social Media Security

1.8 PROTECT YOURSELF AND YOUR DATA WHEN USING SOCIAL NETWORKING SITES¹¹

Online communities have existed since the invention of the internet. First there were bulletin boards and email lists, which gave people around the world opportunities to connect, to communicate and to share information about particular subjects. Today, social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are. These functions are not new or unique – any of these actions can also be performed via the internet without joining a social networking site.

Although these networks can be very useful, and promote social interaction both online and offline, when using them you may be making information available to people who want to abuse it. Think of a social networking site as being like a huge party. There are people there that you know, as well as some that you don't know at all. Imagine walking through the party with all your personal details, and up-to-the-minute accounts of what you are thinking, written on a big sign stuck on your back so that everyone can read it without you even knowing. Do you really want everyone to know all about you?

Remember that social networking sites are owned by private businesses, and that they make their money by collecting data about individuals and selling that data on, particularly to third party advertisers. When you enter a social networking site, you are leaving the freedoms of the internet behind and are entering a network that is governed and ruled by the owners of the site. Privacy settings are only meant to protect you from other members of the social network, but they do not shield your data from the owners of the service. Essentially you are giving all your data over to the owners and trusting them with it.

If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise. Human rights advocates are particularly vulnerable to the dangers of social networking sites and need to be extremely careful about the information they reveal about themselves AND about the people they work with.

¹¹ <https://securityinabox.org/en/guide/social-networking>

Before you use any social networking site it is important to understand how they make you vulnerable, and then take steps to protect yourself and the people you work with. This guide will help you understand the security implications of using social networking sites.

1.8.1 General Tips on using Social Networking platforms safely

Social media have become an evident part of our life. We share out updates with our friends, family and anyone who is concerned using social media. But the hackers can use this information to steal sensitive data and hack your account. Given below are some of the general tips on using social media

- Always ask the questions:
 - ✓ Who can access the information I am putting online?
 - ✓ Who controls and owns the information I put into a social networking site?
 - ✓ What information about me are my contacts passing on to other people?
 - ✓ Will my contacts mind if I share information about them with other people?
 - ✓ Do I trust everyone with whom I'm connected?
- Always make sure you use **secure passwords** to access social networks. If anyone else does get into your account, they are gaining access to a lot of information about you and about anyone else you are connected to via that social network. Change your passwords regularly as a matter of routine.
- Make sure you understand the default **privacy settings** offered by the social networking site, and how to change them.
- Consider using **separate accounts/identities**, or maybe different pseudonyms, for different campaigns and activities. Remember that the key to using a network safely is being able to trust its members. Separate accounts may be a good way to ensure that such trust is possible.
- Be careful when accessing your social network account in public internet spaces. **Delete your password and browsing history** when using a browser on a public machine.
- **Access social networking sites using https://** to safeguard your username, password and other information you post. Using https:// rather than http:// adds another layer of security by encrypting the traffic from your browser to your social networking site.

- Be careful about putting too much information into **your status updates** – even if you trust the people in your networks. It is easy for someone to copy your information.
- Most social networks allow you to integrate information with other social networks. For example you can post an update on your Twitter account and have it automatically posted on your Facebook account as well. Be particularly **careful when integrating your social network accounts!** You may be anonymous on one site, but exposed when using another.
- Be cautious about how safe your content is on a social networking site. **Never rely on a social networking site as a primary host for your content** or information. It is very easy for governments to block access to a social networking site within their boundaries if they suddenly find its content objectionable. The administrators of a social networking site may also decide to remove objectionable content themselves, rather than face censorship within a particular country.

1.8.2 Posting Personal Details

Social networking sites ask you for a good deal of data about yourself to make it easier for other users to find and connect to you. Perhaps the biggest vulnerability this creates for users of these sites is the possibility of identity fraud, which is increasingly common. In addition, the more information about yourself you reveal online, the easier it becomes for the authorities to identify you and monitor your activities. The online activities of diaspora activists from some countries have led to the targeting of their family members by the authorities in their homelands.

Ask yourself: is it necessary to post the following information online?

- ✓ birth dates
- ✓ contact phone numbers
- ✓ addresses
- ✓ details of family members
- ✓ sexual orientation
- ✓ education and employment history

1.8.3 Friends, Followers and Contacts

The first thing you will do after filling in your personal details with any social networking application is establish connections to other people. Presumably these contacts are people you know and trust – but you may also be connecting to an online community of like-minded

individuals that you have never met. The most important thing to understand is what information you are allowing this online community to have.

When using a social network account such as Facebook, where a lot of information about yourself is held, consider only connecting to people you know and trust not to misuse the information you post.

1.8.4 Status Updates

On Twitter and Facebook and similar networks, the status update answers the questions: What am I doing right now? What's happening? The most important thing to understand about the status update is who can actually see it. The default setting for the status update on most social networking applications is that anyone on the internet can see it. If you only want your contacts to see the updates, you need to tell the social networking application to keep your updates hidden from everyone else.

To do this in Twitter, look for “Protect Your Tweets”. In Facebook, change your settings to share your updates with “Friends Only”. Even if you switch to those settings, consider how easy it is for your information to be reposted by followers and friends. Agree with your network of friends on a common approach to passing on the information posted in your social networking accounts. You should also think about what you may be revealing about your friends that they may not want other people to know; it's important to be sensitive about this, and to ask others to be sensitive about what they reveal about you.

There have been many incidents in which information included in status updates has been used against people. Teachers in the US have been fired after posting updates about how they felt about their students; other employees have lost their jobs for posting about their employers. This is something that nearly everyone needs to be careful about.

1.8.5 Sharing Online Content

It's easy to share a link to a website and get your friend's attention. But who else will be paying attention, and what kind of reaction will they have? If you share (or "like") a site that opposes some position taken by your government, for example, agents of that government very might well take an interest and target you for additional surveillance or direct persecution.

If you want your contacts (and of course the administrators of the social networking platform you use) to be the only ones who can see the things you share or mark as interesting, be sure to check your privacy settings.

1.8.6 Revealing your Location

Most social networking sites will display your location if that data is available. This function is generally provided when you use a GPS-enabled phone to interact with a social network, but don't assume that it's not possible if you aren't connecting from a mobile. The network your computer is connected to may also provide location data. The way to be safest about it is to double-check your settings.

Be particularly mindful of location settings on photo and video sharing sites. Don't just assume that they're not sharing your location: double-check your settings to be sure.

1.8.7 Sharing Videos and Photos

Photos and videos can reveal people's identities very easily. It's important that you have the consent of the subject/s of any photo or video that you post. If you are posting an image of someone else, be aware of how you may be compromising their privacy. Never post a video or photo of anyone without getting their consent first.

Photos and videos can also reveal a lot of information unintentionally. Many cameras will embed hidden data (metadata tags), that reveal the date, time and location of the photo, camera type, etc. Photo and video sharing sites may publish this information when you upload content to their sites.

1.8.8 Instant Chats

Many social networking sites have tools that allow you to have discussions with your friends in real time. These operate like Instant Messaging and are one of the most insecure ways to communicate on the internet, both because they may reveal who you are communicating with, and what you are communicating about.

Connecting to the site via https is a minimum requirement for secure chatting, but even this is not always a guarantee that your chat is using a secure connection. For example, Facebook chat uses a different channel to HTTPS (and is more prone to exposure).

It is more secure to use a specific application for your chats, such as Pidgin with an Off-the-record plugin, which uses encryption. Read the 'Pidgin – secure instant messaging' hands-on guide.

1.8.9 Joining and Creating Groups, Events and Communities

What information are you giving to people if you join a group or community? What does it say about you? Alternatively, what are people announcing to the world if they join a group or community that you have created? How are you putting people at risk?

When you join a community or group online it is revealing something about you to others. On the whole, people may assume that you support or agree with what the group is saying or doing, which could make you vulnerable if you are seen to align yourself with particular political groups, for example. Also if you join a group with a large number of members that you don't know, then this can compromise any privacy or security settings that you have applied to your account, so think about what information you are giving away before joining. Are you using your photo and real name so strangers can identify you?

Alternatively, if you set up a group and people choose to join it, what are they announcing to the world by doing so? For example, perhaps it is a gay and lesbian support group that you have set up to help people, but by joining it people are openly identifying themselves as gay or gay-friendly, which could bring about dangers for them in the real world.

ACTIVITY

1. After going through the above section, find out whether you were following the above safe practices while handling your social media account? Find the gaps?
2. Based on the above recommendations, adjust your social media account settings.

RECOMENDED VIDEOS

https://www.youtube.com/watch?v=QUyla_nMJis

<https://www.youtube.com/watch?v=-CeuqCHX7tE>

<https://www.youtube.com/watch?v=xCHTmzfsGmI>

UNIT VIII: Email Security

1.9 EMAIL SECURITY TIPS¹²

- Don't open email attachments that you are not expecting, or which have come from someone you do not know. When you open such an email, make sure that your anti-virus software is up-to-date and pay close attention to any warnings from your browser or email program.
- You can use anonymity software which can help you hide your chosen email service from anyone who might be monitoring your internet connection. A good, free software programme to do this is **Tor** (Find out more about Tor browser using Google). If you don't want to give away information about your identity through your email, do not register a username or 'Full Name' that is related to your personal or professional life.
- You can avoid getting spam (unwanted or junk email) by guarding your email address and distributing it sparingly. Also, never open or reply to any emails you consider to be spam, because spammers will take this as a proof of the legitimacy of the address and will just send you more spam. Consider using a spam filter, but remember that it needs to be monitored as it may mistake a genuine email for spam.
- You should try to avoid your emails being mistaken for spam by the recipients. Spam filters will block messages with certain words in the subject heading. It is worth scanning your spam folder for subject lines that are getting blocked.
- Beware of email scams. Many scam emails pretend to come from a bank, Ebay, Paypal, or other online shops. If you get an email telling you that your account is in danger of being shut down, or that you need to take immediate action by updating your account information, be very suspicious: these messages are usually scams. Another frequent scam has you receiving an email from someone you know which says that they have had an emergency and asks you to send them money. This person's email account is likely to have been compromised by a scammer.
- Pay close attention if your browser suddenly gives you messages about invalid security certificates when you attempt to access a secure webmail account. It could mean that someone is tampering with the communication between your computer and the server in order to intercept your messages.

¹² <https://survival.tacticaltech.org/internet/email/tips>

ACTIVITY

1. What are anonymous accounts? Find some browsers which supports anonymity.

RECOMENDED VIDEOS

<https://www.youtube.com/watch?v=EFHfg1bfgVc>

<https://www.youtube.com/watch?v=tkgLHoaFeFk>

UNIT IX: Smart Phone Security

1.10 SMARTPHONE SECURITY GUIDE¹³

Advances in technology now mean that mobile phones can provide services and features similar to desktop or laptop computers. These Smartphones offer many new ways to communicate and capture and disseminate media. To provide these new functionalities, the smartphones not only use the mobile network, but also connect to the internet either via a wi-fi connection (similar to a laptop at an internet cafe) or via data connections through the mobile network operator.

So while you can, of course, make phone calls with a smartphone, it is better to view smartphones as small computing devices. This means that the other material in this toolkit is relevant to your use of your smartphone as well as your computer.

Smartphones usually support a wide range of functionality – web browsing, email, voice and instant messaging over the internet, capturing, storing and transmitting audio, videos and photos, enabling social networking, multi-user games, banking and many other activities. However, many of these tools and features introduce new security issues, or increase existing risks.

For instance, some smartphones have built-in geo-location (GPS) functionality, which means they can provide your precise location to your mobile network operator by default, and to many applications you use on your phone (such as social networking, mapping, browsing and other applications). As mentioned before, mobile phones already relay your location information to your mobile network operator (as part of the normal functions of the phone). However, the additional GPS functionality not only increases the precision of your location information, it also increases the amount of places where this information might be distributed.

It's worth reviewing all the risks associated with mobile phones discussed in our guide How to use mobile phones as securely as possible as all of them are also relevant to smartphone use. That guide also covers issues of eavesdropping, interception of SMS or phone calls, SIM card related issues, and best practices.

¹³ <https://securityinabox.org/en/guide/smartphones>

In this guide we'll take a look at the additional security challenges posed by smartphones.

1.10.1 Introduction to Smartphone Security

1.10.1.1 Purses, Wallets, Smartphones

We have an intuitive understanding of the value of keeping our purse or wallet safe, because so much sensitive information is stored in them, and losing them will compromise our privacy and safety. People are less aware of the amount of personal information being carried in their smartphones, and consider losing a phone a nuisance rather than a risk. If you also think that a smartphone is a computing device which is always connected to a network and is continually carried around, it also highlights the important difference between a holder of discrete, passive information (like a wallet), and an active and interactive item like a smartphone.

A simple exercise can help illustrate this:

Empty the content of your wallet or purse, and take account of sensitive items. Typically you may find: - Pictures of loved ones (~5 pictures) - Identification cards (driver's license, membership cards, social security cards) - Insurance and health information (~2 cards) - Money (~5 bills) - Credit/Debit cards (~3 cards)

Now, examine the contents of your smartphone. A typical smartphone user may find some of the above in higher quantities, and in some cases much more valuable items:

- Pictures of loved ones (~100 pictures)
- Email applications and their passwords
- Emails (~500 emails)
- Videos (~50 videos)
- Social networking applications and their passwords
- Banking applications (with access to the bank accounts)
- Sensitive documents
- Sensitive communication records
- A live connection to your sensitive information

The more you use smartphones, the more you need to become aware of the associated risks and take appropriate precautions. Smartphones are powerful amplifiers and distributors of your personal data. They are designed to provide as much connectivity as possible and to link

to social networking services by default. This is because your personal data is valuable information that can be aggregated, searched and sold.

It can be disastrous if you lose your phone without having a backup of your most important data (such as your contacts) in a secure location. Besides backing up your data, make sure you also know how to restore the data. Keep a hard copy of the steps you need to take so you can do it quickly in an emergency.

In this chapter we'll start by introducing some smartphone basics – a description of various platforms and some basic setup procedures for securing your information and communication. The remaining parts of this chapter will cover specific precautions related to common uses of smartphones.

1.10.2 Platforms, Setup and Installation

1.10.2.1 Platforms and Operating Systems

At the time of writing, the most common smartphones in use are Apple's iPhone and Google's Android, followed by Blackberry and Windows phones. The key difference between Android and other operating systems is that Android is, mostly, an Open Source (*FOSS*) system, which allows the operating system to be audited independently to verify if it properly protects users' information and communication. It also facilitates development of security applications for this platform. Many security-aware programmers develop Android applications with user safety and security in mind. Some of these will be highlighted later in this chapter.

Regardless what type of smartphone you are using, there are issues that you should be aware of when you use a phone which connects to the internet and comes with features such as *GPS* or wireless networking capacities. In this chapter we focus on devices with the Android platform, because, as mentioned above, it's easier to secure data and communications. Nonetheless, basic setup guides and some applications for devices other than Android phones are provided, too.

Blackberry phones have been presented as “secure” messaging and email devices. This is because messages and emails are securely channeled through Blackberry servers, out of the reach of potential eavesdroppers. Unfortunately, more and more governments are demanding access to these communications, citing need for guarding against potential terrorism and organised crime. India, United Arab Emirates, Saudi Arabia, Indonesia and Lebanon are examples of governments which have scrutinized the use of Blackberry devices and demanded access to user data in their countries.

1.10.2.2 Feature Phones

Another category of mobiles are often called 'feature phones'. Recently, feature phones have increased their functionalities to include those of some smartphones. But generally, feature phones' operating systems are less accessible, therefore there are limited opportunities for security applications or improvements. We do not specifically address feature phones, although many measures discussed here make sense for feature phones too.

1.10.2.3 Branded and locked smartphones

Smartphones are usually sold branded or locked. Locking smartphones means that the device can only be operated with one carrier, whose SIM card is the only one that will work in the device. Mobile network operators usually brand a phone by installing their own firmware or software. They may also disable some functionalities or add others. Branding is a means for companies to increase revenue by channelling your smartphone use, often also collecting data about how you are using the phone or by enabling remote access to your smartphone.

For these reasons, we recommend that you buy an unbranded smartphone if you can. A locked phone poses a higher risk since all your data is routed through one carrier, which centralises your data streams and makes it impossible to change SIM cards to disseminate the data over different carriers. If your phone is locked, ask someone you trust about unlocking it.

1.10.2.4 General Setup

Smartphones have many settings which control the security of the device. It is important to pay attention to how your smartphone is set up. In the Hands-on Guides below we will alert you to certain smartphone security settings that are available but not active by default, as well as those which are active by default and make your phone vulnerable.

1.10.2.5 Installing and updating applications

The usual way to install new software on your smartphone is to use the iPhone Appstore or Google Play store, log in with your user credentials, and download and install a desired application. By logging-in you associate your usage of the online store with the logged-in user account. The owners of the application store keep records of this user's browsing history and application choices.

The applications which are offered in the official online store are, supposedly, verified by store owners (Google or Apple), but in reality this provides weak protection against what applications will do after being installed on your phone. For example, some applications may copy and send out your address book after you install them on your phone. On Android

phones each application needs to request, during the installation process, what it will be permitted to do when it is in use. You should pay close attention to what permissions are requested, and if these permissions make sense for the function of the app you are installing. For example, if you are considering a "news reader" application and you find out that it requests the rights to send your contacts over a mobile data connection to a third party, you should look for alternative applications with appropriate access and rights. Sites. Some users may want to consider these alternative sites to minimize online contact with Google. One of the alternative store is **F-Droid** ('Free Droid'), which only provides FOSS applications. However please remember that you should trust the site before you download any apps from it. For inexperienced users we recommend that you use Google Play store.

If you don't want to (or are unable to) go online to access apps, you can transfer apps from someone else's phone by sending .apk files (short for 'android application package') via bluetooth. Alternatively you could download the .apk file to your device's Micro SD card or use a usb cable to move it there from a PC. When you have received the file, simply long tap on the filename and you will be prompted to install it. (**Note:** be especially careful while using Bluetooth).

1.10.3 Communicating Securely(Through Voice and Messages) with a Smartphone

1.10.3.1 Secure Voice Communication

Basic telephony

In order to send or receive any calls or communications to your phone, the signal towers nearest you are alerted by your phone of its presence¹⁴. As a result of those alerts and communications the network service provider knows the precise geographic location of your mobile phone at any given time.

About Anonymity: If you are conducting sensitive phone conversations or sending sensitive SMS messages, beware of the above tracking 'feature' of all mobile phones. Consider adopting the steps below:

- Make calls from different locations each time, and choose locations that are not associated with you.
- Keep your phone turned off, with the battery disconnected, go to the chosen location, switch your phone on, communicate, switch the phone off and disconnect the battery.

¹⁴ <https://securityinabox.org/en/guide/mobile-phones>

Doing this habitually, each time you have to make a call, will mean that the network cannot track your movements.

- Change phones and SIM cards often. Rotate them between friends or the second-hand market.
- Use unregistered pre-paid SIM cards if this is possible in your area. Avoid paying for a phone or SIM cards using a credit card, which will also create a connection between these items and you.

About eavesdropping: Your phone can be set to record and transmit any sounds within the range of its microphone without your knowledge. Some phones can be switched on remotely and brought into action in this way, even when they look as though they are switched off.

- Never let people whom you don't trust get physical access to your phone; this is a common way of installing spying software on your phone.
- If you are conducting private and important meetings, switch your phone off and disconnect the battery. Or don't carry the phone with you if you can leave it where it will be absolutely safe.
- Make sure that any person with whom you communicate also employs the safeguards described here.
- In addition, don't forget that using a phone in public, or in places that you don't trust, makes you vulnerable to traditional eavesdropping techniques, or to having your phone stolen.

About interception of calls: Typically, encryption of voice communications (and of text messages) that travel through the mobile phone network is relatively weak. There are inexpensive techniques which third parties can use to intercept your written communications, or to listen to your calls, if they are in proximity to the phone and can receive transmissions from it. And of course, mobile phone providers have access to all your voice and text communications. It is currently expensive and/or somewhat technically cumbersome to encrypt phone calls so that even the mobile phone provider can't eavesdrop – however, these tools are expected to become cheaper soon. To deploy the encryption you would first have to install an encryption application on your phone, as well as on the device of the person with whom you plan to communicate. Then you would use this application to send and receive encrypted calls and/or messages. Encryption software is currently only supported on a few models of so-called 'smart' phones.

Conversations between Skype and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place¹⁵. Using Internet through your Smartphone over mobile data connections or WiFi can provide more secure ways to communicate with people, namely by using VoIP and employing means to secure this channel of communication. Some smartphone tools can even extend some of this security beyond VoIP, to mobile phone calls as well (See **Redphone** below).

Here we list a few tools and their pros and cons:

Skype

The most popular commercial VoIP application, Skype, is available for all smartphone platforms and works well if your wireless connectivity is reliable. It is less reliable on mobile data connections.

Skype is a non Open-Source software what makes it very difficult to independently confirm its level of security. Additionally, Skype is owned by Microsoft, which has a commercial interest in knowing when you use Skype and from where. Skype also may allow law enforcement agencies retrospective access to all your communications history.

Other VoIP tools

Using VoIP is generally free (or significantly cheaper than mobile phone calls) and leaves few data traces. In fact, a secured VoIP call can be the most secure way to communicate.

RedPhone is a Free and Open-Source Software application that encrypts voice communication data sent between two devices that run this application. It is easy to install and very easy to use, since it integrates itself into your normal dialing and contact scheme. But people you want to talk to also need to install and use RedPhone. For ease of use, RedPhone uses your mobile number as a way to identify you to your contacts. Unfortunately, this makes it more difficult to use RedPhone without a functioning mobile service plan, even on devices capable of using WiFi to connect to the Internet. RedPhone also uses a central server, which puts the administrators of the service in a powerful position by allowing them to see much of the meta-data related to your encrypted VoIP calls.

CSipSimple is a powerful VoIP client for Android phones that is well maintained and comes with many easy set-up wizards for different VoIP services.

¹⁵ <https://securityinabox.org/en/guide/smartphones>

Open Secure Telephony Network (OSTN) and the server provided by the Guardian project, **ostel.co**, currently offers one of the most secure means to communicate via voice. Knowing and trusting the entity that operates the server for your VoIP communication needs is an important consideration.

When using CSipSimple, you never directly communicate with your contact, instead all your data is routed through the Ostel server. This makes it much harder to trace your data and find out who you are talking to. Additionally, Ostel doesn't retain any of this data, except the account data that you need to log in. All your speech is securely encrypted and even your meta data, which is usually very hard to disguise, is blurred since traffic is proxied through the ostel.co server. If you download CSipSimple from ostel.co it also comes preconfigured for use with ostel, which makes it very easy to install and use.

Tool Guides for CSipSimple and Ostel.co are forthcoming. In the meantime, more information can be found by following the links above.

1.10.3.2 Sending Messages Securely

You should use precautions when sending SMS and using instant messaging or chatting on your smartphone.

SMS

SMS communication is insecure by default. Anyone with access to a mobile telecommunication network can intercept these messages easily and this is an everyday occurrence in many situations. Don't rely on sending unsecured SMS messages in critical situations. There is also no way of authenticating SMS messages, so it is impossible to know if the contents of a message was changed during delivery or if the sender of the message really is the person they claim to be.

Securing SMS

TextSecure is a *FOSS* tool for sending and receiving secure SMS on Android phones. It works both for encrypted and non-encrypted messages, so you can use it as your default SMS application. To exchange encrypted messages this tool has to be installed by both the sender and the recipient of a message, so you will need to get people you communicate with regularly to use it as well. TextSecure automatically detects when an encrypted message is received from another TextSecure user. It also allows you to send encrypted messages to more than one person. Messages are automatically signed making it nearly impossible to

tamper with the contents of a message. In our TextSecure hands-on guide we explain in detail the features of this tool and how to use it.

Secure Chat

Instant messaging and chatting on your phone can produce a lot of information that is at risk of interception. These conversations might be used against you by adversaries at a later date. You should therefore be extremely wary about what you reveal when you are writing on your phone while instant messaging and chatting.

There are ways to chat and instant message securely. The best way is to use end-to-end encryption, as this will enable you to make sure the person on the other end is who you want.

We recommend ChatSecure as a secure text chat application for the Android phones. ChatSecure offers easy and strong encryption for your chats with *Off-the-Record* Messaging protocol. This encryption provides both authenticity (you can verify that you are chatting with the right person) and the independent security of each session so that even if the encryption of one chat session is compromised, other past and future sessions will remain secure.

ChatSecure has been designed to work together with Orbot, so your chat messages can be routed through the *Tor* anonymizing network. This makes it very hard to trace it or even find out that it happened.

For iPhones, the **ChatSecure** client provides the same features, although it is not easy to use it with the *Tor* network.

Whichever application you will use always consider which account you use to chat from. For example when you use Google Talk, your credentials and time of your chatting session are known to Google. Also agree with your conversation partners on not saving chat histories, especially if they aren't encrypted.

1.10.3.3 Storing Information on your Smartphone

Smartphones come with large data storage capacities. Unfortunately, the data stored on your device can be easily accessible by third parties, either remotely or with physical access to the phone. You can take steps to encrypt any sensitive information on your phone by using specific tools.

Date Encryption Tools

The **Android Privacy Guard (APG)** allows OpenPGP encryption for files and emails. It can be used to keep your files and documents safe on your phone, as well when emailing.

Recording Password Securely

You can keep all your needed passwords in one secure, encrypted file by using **Keepass**. You will only need to remember one master password to access all the others. With Keepass you can use very strong passwords for each account you have, as Keepass will remember them for you, and it also comes with a password generator to create new passwords. You can synchronise Keepass password databases between your phone and your computer. We recommend that you synchronise only those passwords that you will actually use on your mobile phone. You can create a separate smaller password database on the computer and synchronise this one instead of copying an entire database with all the passwords that you use to your smartphone. Also, since all the passwords are protected by your master password, it is vital to use very strong password for your Keepass database.

1.10.3.4 Sending Email from your Smartphone

In this section we will briefly discuss the use of email on smartphones. In the first instance, consider if you really need to use your smartphone to access your email. Securing a computer and its content is generally simpler than doing so for a mobile device such as a smartphone. A smartphone is more susceptible to theft, monitoring and intrusion.

If it is absolutely vital that you access your email on your smartphone, there are actions you can take to minimize the risks.

- Do not rely on smartphone as your primary means for accessing your email. Downloading (and removing) emails from an email server and storing them only on your smartphone is not advised. You can set up your email application to use only copies of emails.
- If you use email encryption with some of your contacts, consider installing it on your smartphone, too. The additional benefit is that encrypted emails will remain secret if the phone falls into wrong hands.

Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks. Consider creating a mobile-only encryption key-pair (using **APG**) for your use on your smartphone, so you do not copy your encryption private key from your computer to the mobile device. Note that this requires that you ask people you communicate with to also encrypt emails using your mobile-only encryption key.

1.10.3.5 Capturing Media with your Smartphone

Capturing pictures, video or audio with your Smartphone can be a powerful means to document and share important events. However, it is important to be careful and respectful of privacy and safety of those pictured, filmed or recorded. For example, if you take photos or record video or audio of an important event, it might be dangerous to you or to those who appear in the recordings, if your phone fell into the wrong hands. In this case, these suggestions may be helpful:

- Have a mechanism to securely upload recorded media files to protected online location and remove them from the phone instantly (or as soon as you can) after recording.
- Use tools to blur the faces of those appearing in the images or videos or distort the voices of audio or videos recordings and store only blurred and distorted copies of media files on your mobile device.
- Protect or remove meta information about time and place within the media files.

Guardian Project has created a *FOSS* app called **ObscuraCam** to detect faces on photos and blur them. You can choose the blurring mode and what to blur, of course. Obscuracam also deletes the original photos and if you have set up a server to upload the captured media, it provides easy functionality to upload it.

1.10.3.6 Accessing the Internet Securely from your Smartphone

As discussed in our guide **How to keep your Internet communication private** and our guide **How to remain anonymous and bypass censorship on the Internet**, access to content on the Internet, or publishing material online such as photos or videos, leaves many traces of who and where you are and what you are doing. This may put you at risk. Using your smartphone to communicate with the Internet magnifies this risk.

Through Wi-Fi or Mobile Data

Smartphones allow you to control how you access the Internet: via a wireless connection provided by an access point (such as an internet cafe), or via a mobile data connection, such as GPRS, EDGE, or UMTS provided by your mobile network operator.

Using a WiFi connection reduces the traces of data you may be leaving with your mobile phone service provider (by not having it connected with your mobile phone subscription). However, sometimes a mobile data connection is the only way to get online. Unfortunately mobile data connection protocols (like EDGE or UMTS) are not open standards. Independent

developers and security engineers cannot examine these protocols to see how they are being implemented by mobile data carriers.

In some countries mobile access providers operate under different legislation than internet service providers, which can result in more direct surveillance by governments and carriers.

Regardless of which path you take for your digital communications with a smartphone, you can reduce your risks of data exposure through the use of anonymising and encryption tools.

Anonymity of your Smartphone

To access content online anonymously, you can use an Android app called **Orbot**. Orbot channels your internet communication through Tor's anonymity network.

Another app, Orweb, is a web browser that has privacy enhancing features like using proxies and not keeping a local browsing history. Orbot and Orweb together circumvent web filters and firewalls, and offer anonymous browsing.

Proxies

The mobile version of *Firefox* – **Firefox mobile** can be equipped with proxy add-ons, which direct your traffic to a proxy server. From there your traffic goes to the site you are requesting. This is helpful in cases of censorship, but still may reveal your requests unless the connection from your client to the proxy is encrypted. We recommend the **Proxy Mobile** add-on (also from **Guardian Project**, which makes proxying with Firefox easy. Is also the only way to channel Firefox mobile communications to Orbot and use the *Tor* network.

1.10.3.7 Advanced Smart Phone Security

Get Full Access to your Smartphone

Most Smartphones are capable of more than their installed operating system, manufacturers' software (firmware), or the mobile operators' programmes allow. Conversely, some functionalities are 'locked in' so the user is not capable of controlling or altering these functions, and they remain out of reach. In most cases those functionalities are unnecessary for smartphone users. There are however, some applications and functionalities that can enhance the security of data and communications on a smartphone. Also there are some other existing functionalities that can be removed to avoid security risks.

For this, and other reasons, some smartphone users choose to manipulate the various software and programs running the smartphone in order to gain appropriate privileges to allow them to install enhanced functionalities, or remove or reduce other ones.

The process of overcoming the limits imposed by mobile carriers, or manufacturers of operating systems on a smartphone is called rooting (in case of Android devices), or jailbreaking (in case of iOS devices, like iPhone or iPad). Typically, successful rooting or jailbreaking will result in your having all the privileges needed to install and use additional applications, make modifications to otherwise locked-down configurations, and total control over data storage and memory of the smartphone.

WARNING: Rooting or jailbreaking may not be a reversible process, and it requires experience with software installation and configuration. Consider the following:

- There is a risk of making your smartphone permanently inoperable, or 'bricking' it (i.e. turning it into a 'brick').
- The manufacturer or mobile carrier warranty may be voided.
- In some places, this process maybe illegal.

But if you are careful, a rooted device is a straightforward way to gain more control over your smartphone to make it much more secure.

Alternative Firmwares

Firmware refers to programmes that are closely related to the particular device. They are in cooperation with the device's operating system and are responsible for basic operations of the hardware of your smartphone, such as the speaker, microphone, cameras, touchscreen, memory, keys, antennas, etc.

If you have an Android device, you might consider installing a firmware alternative to further enhance your control of the phone. Note that in order to install alternative firmware, you need to root your phone.

An example of an alternative firmware for an Android phone is **Cyanogenmod** which, for example, allows you to uninstall applications from the system level of your phone (i.e. those installed by the phone's manufacturer or your mobile network operator). By doing so, you can reduce the number of ways in which your device can be monitored, such as data that is sent to your service provider without your knowledge.

In addition, Cyanogenmod ships by default with an OpenVPN application, which can be tedious to install otherwise. VPN (Virtual Private Network) is one of the ways to securely proxy your internet communication (see below).

Cyanogenmod also offers an Incognito browsing mode in which history of your communication is not recorded on your smartphone.

Full Device Encryption

If your phone is rooted you may consider encrypting its entire data storage or creating a volume on the Smartphone to protect some information on the phone.

Luks Manager allows easy, on-the-fly strong encryption of volumes with an user-friendly interface. We highly recommend that you install this tool before you start storing important data on your Android device and use the Encrypted Volumes that the Luks Manager provides to store all your data.

Virtual Private Network(VPN) Security

A VPN provides an encrypted tunnel through the internet between your device and a VPN server. This is called a tunnel, because unlike other encrypted traffic, like https, it hides all services, protocols, and contents. A VPN connection is set up once, and only terminates when you decide.

Note that since all your traffic goes through the proxy or VPN server, an intermediary only needs to have access to the proxy to analyze your activities. Therefore it is important to carefully choose amongst proxy services and VPN services. It is also advisable to use different proxies and/or VPNs since distributing your data streams reduces the impact of a compromised service.

ACTIVITIES

1. Find out more about jailbreaking over internet.
2. Find and use the feature of “off-the –record” option in your chat application and observe what difference it makes.
3. Download and use Skype to make a video call to your friend.
4. Find out more about ***ObscuraCam*** over internet.

RECOMENDED VIDEOS

<https://www.youtube.com/watch?v=KCObM4PBTvk>

<https://www.youtube.com/watch?v=V8bCyRCqK0k>

UNIT X: How to secure your Computer using Antivirus

1.11 SECURING COMPUTER USING FREE ANTIVIRUS¹⁶

As computers become more and more integrated in to our lives, we end up leaving many sensitive data on our computer-from passwords, official email id, bank account to personal notes, business plans and other confidential information. So, good security software is a must for everyone. Here is a list of 11 free anti-virus software and its common features which you can select (home users) for your online security. All are listed in alphabetical order

1. Avast Antivirus– Avast is one of the best free anti-virus software available that provides a complete protection against security threats. This full-featured antivirus package has the following feature: Built in Anti-spyware, Anti-Rootkit, Web shield, Strong self protection, P2P and IM shield, Anti-Virus kernel, resident protection, Network shield, Automatic update, System integration, Windows 64 bit support, Integrated Virus Cleaner. It can be downloaded from <https://www.avast.com/index>

2. AVG Antivirus – AVG anti-virus free edition provides basic antivirus and anti-spyware protection for Windows. Following features included in the free edition: Anti-virus , anti-spyware and Safe surf feature. It can be downloaded from <http://free.avg.com/>

3. Avira AntiVir Personal - Avira is a comprehensive, easy to use antivirus program, designed to reliable free of charge virus protection to home-users. Features included are: Protection from virus worms and Trojans, Anti-rootkit, Anti-fishing, Anti dialers. It can be downloaded from <http://www.free-av.com/>

4. BitDefender - Free Edition uses the same ICSA Labs certified scanning engines found in Pro version of BitDefender , allowing you to enjoy basic virus protection for no cost at all. Features includes: On demand Virus Scanner and Remover and Scheduled scanning. It can be downloaded from <http://www.bitdefender.com/PRODUCT-14-en--BitDefender-Free-Edition.html>

5. Blink Personal – An all-in one security suite with antivirus limited for one year. Blink personal Security suite features – Antivirus and Anti spyware, Anti root kit, Built-in Firewall protection and Identity protection. It can be downloaded from <http://free-antivirus.eeye.com/>

6. Calmwin antivirus–An open source, free Antivirus program for Windows 98/Me/2000/XP/2003 and Vista. Features include - high detection rates for viruses and spyware; automatic downloads of regularly updated Virus Database, Standalone virus scanner. It does not include an on-access real-time scanner. It can be downloaded from

¹⁶ http://shaifulaueo.blogspot.in/p/free-antivirus_13.html

<http://www.clamwin.com/>

7. Comodo Antivirus - has all the functionality of a paid AV without the price – Features includes- Detects and remove viruses from computers and networks. On Access Scanning conducts a real-time, scheduled virus scan. Host Intrusion Detection allows you to Intercept viruses, spyware, and other malware before they infect your computer. Get updates of the latest virus definitions everyday so you can stay protected against the latest threats. It can be downloaded from <http://antivirus.comodo.com/>

8. Moon Secure Antivirus - Aims to be the best Free Antivirus for Windows under GPL license. It offers multiple scan engines, Net shield, Firewall, On access, on Exec scanner and rootkits preventions plus features from Commercial Antivirus applications. It can be downloaded from <http://sourceforge.net/projects/moonav/>

9. PCTools Antivirus- with PC Tools AntiVirus Free Edition you are protected against the most nefarious cyber-threats attempting to gain access to your PC and personal information. It protects you from Virus, worm, Trojan and has Smart Updates, IntelliGuard Protection, file guard and email guard. It can be downloaded from <http://www.pctools.com/free-antivirus/>

10. Rising Antivirus – Rising Antivirus Free Edition is a solution with no cost to personal users for the life of the product while still provides the same level of detection and protection capability as RISING Antivirus . It protects your computers against all types of viruses, Trojans, worms, rootkits and other malicious programs. Ease of use and Smartupdate technology make it an "install and forget" product and entitles you to focus on your own jobs with your computer. It can be downloaded from <http://www.freerav.com/>

11. Threatfire Lite – Provides Comprehensive protection against viruses, worms, Trojans, spyware, rootkits, keyloggers & buffer overflows. And have Real-time behavior-based malware detection, malware quarantine & removal, etc. It can be downloaded from <http://www.threatfire.com/download/>

ACTIVITY

1. Compare the feature of some of the popular free antiviruses.
2. What is the difference between free antivirus and paid antivirus? Is it safe to use free antivirus in your machine?

RECOMENDED VIDEOS

<https://www.youtube.com/watch?v=WprjZyY8ZuY>

<https://www.youtube.com/watch?v=mYhJyVKjai4>

<https://www.youtube.com/watch?v=MFyPg2Flf8s>

<https://www.youtube.com/watch?v=iNWUtj9qhPo>

<https://www.youtube.com/watch?v=A9O0zYv-5d0>

https://www.youtube.com/watch?v=cdRbvO_MXh4

UNIT XI: Use of Encryption technologies for securing data

1.12 PROTECTING THE SENSITIVE FILES ON YOUR COMPUTER¹⁷

Unauthorised access to the information on your computer or portable storage devices can be carried out remotely, if the 'intruder' is able to read or modify your data over the Internet; or physically, if he manages to get hold of your hardware. It is always best to have several layers of defence, however, which is why you should also protect the files themselves. That way, your sensitive information is likely to remain safe even if your other security efforts prove inadequate.

There are two general approaches to the challenge of securing your data in this way. You can *encrypt* your files, making them unreadable to anyone but you, or you can hide them in the hope that an intruder will be unable to find your sensitive information. There are tools to help you with either approach, called *TrueCrypt*, which can both *encrypt* and hide your files.

1.12.1 Introduction to Secure File Storage

1.12.1.1 Encrypting your Information

Encrypting your information is a bit like keeping it in a locked safe. Only those who have a key or know the lock's combination (an encryption key or password, in this case) can access it. The analogy is particularly appropriate for *TrueCrypt* and tools like it, which create secure containers called 'encrypted volumes' rather than simply protecting one file at a time. You can put a large number of files into an *encrypted* volume, but these tools will not protect anything that is stored elsewhere on your computer or USB memory stick.

While other software can provide similar strength encryption, *TrueCrypt* contains several important features to allow you to design your information security strategy. It offers the possibility of permanently **encrypting the whole disk of your computer** including all your files, all temporary files created during your work, all programs you have installed and all Windows operating system files. *TrueCrypt* supports encrypted volumes on portable storage devices. It provides 'deniability' features described in the Hiding your sensitive information section below. In addition *TrueCrypt* is a free and open source program.

1.12.1.2 Tips on using File Encryption Safely

Storing confidential data can be a risk for you and for the people you work with. Encryption reduces this risk but does not eliminate it. The first step to protecting sensitive information is to reduce how much of it you keep around. Unless you have a good

¹⁷ <https://securityinabox.org/en/guide/secure-file-storage>

reason to store a particular file, or a particular category of information within a file, you should simply delete it (see How to destroy sensitive information for more information about how to do this securely). The second step is to use a good file encryption tool, such as TrueCrypt.

Returning to the analogy of a locked safe, there are a few things you should bear in mind when using TrueCrypt and tools like it. No matter how sturdy your safe is, it won't do you a whole lot of good if you leave the door open. When your TrueCrypt volume is 'mounted' (whenever you can access the contents yourself), your data may be vulnerable, so you should keep it closed except when you are actually reading or modifying the files inside it.

There are a few situations when it is especially important that you remember not to leave your encrypted volumes mounted:

- Disconnect them when you walk away from your computer for any length of time. Even if you typically leave your computer running overnight, you need to ensure that you do not leave your sensitive files accessible to physical or remote intruders while you are gone.
- Disconnect them before putting your computer to sleep. This applies to both 'suspend' and 'hibernation' features, which are typically used with laptops but may be present on desktop computers as well.
- Disconnect them before allowing someone else to handle your computer. When taking a laptop through a security checkpoint or border crossing, it is important that you disconnect all encrypted volumes and shut your computer down completely.
- Disconnect them before inserting an untrusted USB memory stick or other external storage device, including those belonging to friends and colleagues.
- If you keep an encrypted volume on a USB memory stick, remember that just removing the device may not immediately disconnect the volume. Even if you need to secure your files in a hurry, you have to dismount the volume properly, then disconnect the external drive or memory stick, then remove the device. You might want to practice until you find the quickest way to do all of these things.

If you decide to keep your TrueCrypt volume on a USB memory stick, you can also keep a copy of the TrueCrypt program with it. This will allow you to access your data on other people's computers. The usual rules still apply, however: if you don't trust the machine to be free of malware, you probably shouldn't be typing in your passwords or accessing your sensitive data.

1.12.2. Hiding your Sensitive Information

One issue with keeping a safe in your home or office, to say nothing of carrying one in your pocket, is that it tends to be quite obvious. Many people have reasonable concerns about incriminating themselves by using *encryption*. Just because the legitimate reasons to *encrypt* data outnumber the illegitimate ones does not make this threat any less real. Essentially, there are two reasons why you might shy away from using a tool like *TrueCrypt*: the risk of self-incrimination and the risk of clearly identifying the location of your most sensitive information.

1.12.2.1 Considering the risk of Self-Incrimination

Encryption is illegal in some countries, which means that downloading, installing or using software of this sort might be a crime in its own right. And, if the police, military or intelligence services are among those groups from whom you are seeking to protect your information, then violating these laws can provide a pretext under which your activities might be investigated or your organisation might be persecuted. In fact, however, threats like this may have nothing to do with the legality of the tools in question. Any time that merely being associated with *encryption* software would be enough to expose you to accusations of criminal activity or espionage (regardless of what is actually inside your *encrypted* volumes), then you will have to think carefully about whether or not such tools are appropriate for your situation.

If that is the case, you have a few options:

- You can avoid using data security software entirely, which would require that you store only non-confidential information or invent a system of code words to protect key elements of your sensitive files.
- You can rely on a technique called *steganography* to hide your sensitive information, rather than encrypting it. There are tools that can help with this, but using them properly requires very careful preparation, and you still risk incriminating yourself in the eyes of anyone who learns what tool you have used.
- You can try to store all of your sensitive information in a secure webmail account, but this demands a reliable network connection and a relatively sophisticated understanding of computers and Internet services. This technique also assumes that network *encryption* is less incriminating than file *encryption* and that you can avoid accidentally copying sensitive data onto your hard drive and leaving it there.

- You can keep sensitive information off of your computer by storing it on a USB memory stick or portable hard drive. However, such devices are typically even more vulnerable than computers to loss and confiscation, so carrying around sensitive, unencrypted information on them is usually a very bad idea.

If necessary, you can employ a range of such tactics. However, even in circumstances where you are concerned about self-incrimination, it may be safest to use *TrueCrypt* anyway, while attempting to disguise your *encrypted* volume as best you can.

If want to make your encrypted volume less conspicuous, you can rename it to look like a different type of file. Using the '.iso' file extension, to disguise it as a CD image, is one option that works well for large volumes of around 700 MB. Other extensions would be more realistic for smaller volumes. This is a bit like hiding your safe behind a painting on the wall of your office. It might not hold up under close inspection, but it will offer some protection. You can also rename the *TrueCrypt* program itself, assuming you have stored it as you would a regular file on your hard drive or USB memory stick, rather than installing it as a program.

1.12.2.2. Considering the risk of Identifying your sensitive Information

Often, you may be less concerned about the consequences of 'getting caught' with *encryption* software on your computer or USB memory stick and more concerned that your encrypted volume will indicate precisely where you store the information that you most wish to protect. While it may be true that no one else can read it, an intruder will know that it is there, and that you have taken steps to protect it. This exposes you to various non-technical methods through which that intruder might attempt to gain access, such as intimidation, blackmail, interrogation and torture. It is in this context that *TrueCrypt's* deniability feature, which is discussed in more detail below, comes into play.

TrueCrypt's deniability feature is one of the ways in which it goes beyond what is typically offered by file *encryption* tools. This feature can be thought of as a peculiar form of *steganography* that disguises your most sensitive information as other, less sensitive, hidden data. It is analogous to installing a subtle 'false bottom' inside that not-so-subtle office safe. If an intruder steals your key, or intimidates you into giving her the safe's combination, she will find some convincing 'decoy' material, but not the information that you truly care about protecting.

Only you know that your safe contains a hidden compartment in the back. This allows you to 'deny' that you are keeping any secrets beyond what you have already given to the intruder,

and might help protect you in situations where you must reveal a password for some reason. Such reasons might include legal or physical threats to your own safety, or that of your colleagues, associates, friends and family members. The purpose of deniability is to give you a chance of escaping from a potentially dangerous situation even if you choose to continue protecting your data. As discussed in the Considering the risk of self-incrimination section above, however, this feature is much less useful if merely being caught with a safe in your office is enough to bring about unacceptable consequences.

TrueCrypt's deniability feature works by storing a 'hidden volume' inside your regular *encrypted* volume. You open this hidden volume by providing an alternate password that is different from the one you would normally use. Even if a technically sophisticated intruder gains access to the standard volume, he will be unable to prove that a hidden one exists. Of course, he may very well know that *TrueCrypt* is capable of hiding information in this way, so there is no guarantee that the threat will disappear as soon as you reveal your decoy password. Plenty of people use *TrueCrypt* without enabling its deniability feature, however, and it is generally considered impossible to determine, through analysis, whether or not a given *encrypted* volume contains this kind of 'false bottom'. That said, it is your job to make sure that you do not reveal your hidden volume through less technical means, such as leaving it open or allowing other applications to create shortcuts to the files that it contains.

ACTIVITIES

1. What is *TrueCrypt*? Why it is used?
2. Using *TrueCrypt* encrypt the D drive of your computer.
3. What are the popular applications available to hide sensitive information in your computer?
4. What is Steganography? Find some tools for Steganography.

UNIT XII: Patching and updating Computer systems

1.13 WHAT IS A SOFTWARE PATCH?¹⁸

A patch is a record of changes made to a set of resources. Typically a patch will add a new feature, fix a bug, or add documentation to the project. A popular means of creating a patch is by using diff, a tool that is commonly available on Linux and Unix systems.

Patches are often the preferred way to submit contributions to open development projects such as open source software, particularly when a project is using a centralised version control system (VCS) and the contributor does not have commit rights. Projects using a distributed version control system (DVCS) may prefer contributions to be submitted as pull requests.

When using patches, the contributor creates a patch and submits it to the project. The project maintainer can then inspect the changes and apply them to the main code base if they so choose. Various tools are available to help with patches. These tools make it very easy to create and manage patches for project outputs such as source code and documentation. Patches and patch management tools are the key to building an active community of contributors to an open development project.

This section provides a simple overview of a software patch. It does not deal with the mechanics of creating and processing patches, which are better handled by the documentation of the patch management tool chosen. In the further reading section, we list a few tools to help you get started with creating patches.

1.13.1 Creating a Patch

When a contributor makes a change to the outputs of a project they do so by editing files available in a version control system. A version control system tracks changes to documents and source code over time. Using one makes creating a patch simple because you can always refer to the version of the source code the changes are based upon. However, there are a few steps that should be taken to maximise the chances of the patch being accepted by the maintainers of a project.

It is important that the contributor ensures that the patch complies with any documentation and coding standards adopted by the project. It is also critical to thoroughly test changes against any test suites the project provides. Finally, each contribution should be clearly documented with, at a minimum, details on:

¹⁸ <http://oss-watch.ac.uk/resources/softwarepatch>

- what it is intended to do
- how it is implemented
- how it is used

Once the contributor is satisfied that the patch is worthy of consideration by the project maintainers, a patch must be created.

How the contributor creates the patch depends on which development environment they are using and on which version control system the project is using. Most Integrated Development Environments (IDEs) include a feature to generate a patch. There are also many tools you can install, providing command line or GUI interfaces to patch generation tools.

After running the chosen tool, one or more files will be produced. Collectively, these files describe the changes made in the contribution. Often multiple files will be placed into a single archive file for ease of management. This archive is called a patch. It is this patch that a contributor submits to the project.

The actual submission process varies from project to project, but in all cases there will be a requirement to address the assignment of copyright or rights to use the IP contained within the patch.

1.13.2 Applying a Patch

Once a patch has been submitted by a contributor, it is then the responsibility of the project maintainers to evaluate and, where appropriate, apply the patch. Different projects have different approaches to reviewing and applying patches. However, they all have some common steps:

- quickly evaluate the value of the patch
- prepare prompt and accurate feedback to the contributor (requesting a resubmission where appropriate)
- experimentally apply the patch
- run any test suites against changed code
- report any problems to the contributor and request a resubmission
- commit the patch to the version control system

Skilled developers can read patch files and understand their implications without actually applying them to the code base. This makes it easy to provide rapid feedback to the

contributor. Should the project maintainer feel that the patch looks like a solid contribution, they will apply it to their local development copy and test it. Since a good contribution will already have undergone extensive testing, this should be a simple matter for the maintainer. However, mistakes can be made and so further testing should always be carried out.

Once a patch is ready to be applied to the version control tree, the maintainer will ‘commit’ it. That is, they will make it available in the public version control system. This action will usually result in an automated notification to the developer community via a ‘commit’ email list. At this point, the wider community is given the opportunity to review the contribution; if the change is in response to a bug report or a feature request, the associated ticket in the issue tracker should be updated.

1.13.3 Is It Really That Simple?

For things to work as smoothly as described above, it is important that contributors create patches against a recent version of the project outputs (usually software code), preferably the most recent version, from the ‘head’ of the version control system. This is because, as time passes, code will evolve. If the code in question has changed since the contributor downloaded their copy, applying the patch may not be as simple as described above, since there may be conflicting changes.

Since users often want to work with a stable version of the code in a production environment, it is possible that the initial changes were not made against the latest development version of software. This creates a dilemma for the contributor: do they contribute a patch against an old version of the code, or do they invest the time in creating a patch against the latest development version?

In order to maximise the chances of a patch being accepted, the contributor should submit the patch against the latest development version. Therefore the contributor should have a development copy of the project deployed and ready to test against. All contributions should first be applied to this development version, and any further changes necessary to ensure it works as expected should be made.

Having a development environment deployed like this has the added benefit of allowing the organisation to test current development versions in a non-critical environment. This, in turn, helps with the decision to upgrade or not when a new release is available.

Failure of contributors to create patches against the latest development version of a project will increase the amount of time a maintainer needs to invest in reviewing and applying the

patch. Consequently, the chances of its being accepted are significantly reduced. Rejection will not prevent the contributor's organisation from using the patch, but it will mean that an upgrade to future releases is made more complicated, since their local modifications will have to be reapplied to new releases. Consequently, putting the effort in at an early stage will reduce the effort to upgrade and thus make it more likely that an upgrade will go smoothly.

Even though it is advisable for contributors to work against the latest development resources, projects should still be willing to consider patches against older versions. A patch against an old version is better than no patch at all. Whether such a patch is applied or not depends on the community and on the perceived value of the patch. An important feature addition or a bug fix is likely to be applied, whereas a niche feature may be ignored as there may be no active developers with a need for that feature.

1.13.3.1 Release Early, Release Often

To minimise the chances of users submitting patches against an outdated release, open development projects should release early and release often. In the early stages of a project, the more frequent the project releases are, and the easier the upgrade path, the more likely users are to move to a new version. Consequently, they are more likely to provide patches against a more recent code base. Looking after users in this way ensures that the project enables users to become valuable contributors with minimal effort.

1.1.3.4 Why Should I Contribute A Patch?

Some people wonder why they should put the effort into providing a patch. They may consider it additional work over and above the development effort of making the modifications in the first place. However, there is purely selfish benefit in creating and submitting a quality patch: it makes it easier to maintain your use of the project outputs.

At some point in the future an organisation is likely to want to use the latest and greatest release of the project outputs. If that organisation's staff has failed to work with the community in order to have their local modifications accepted, they will need to reapply all changes, or lose them. That is, the organisation will be paying its staff to make each change twice.

It is easy to ignore this fact. After all, each change seems insignificant and easy to reapply. However, each change is cumulative, and since the project has been progressing independently of your changes, it is quite possible that the application of your modifications will no longer be a simple activity.

Submitting a patch to a project does not guarantee that it will be included, but it certainly increases the chances, especially if staff are encouraged to work with project maintainers to ensure the patch is compatible with the objectives of the project. It is rare for projects to refuse patches outright; any refusal is usually accompanied by recommendations for ways to make it acceptable to the community.

Ultimately, the act of providing patches to projects ensures that an organisation has a cheaper upgrade path and it makes it easier to create releases. At the same time, they help to ensure that the software they depend on remains in active development.

ACTIVITY

1. Download and install Software patch for your operating system.
2. Download and install Software patch for your antivirus system.

RECOMENDED VIDEOS

<https://www.youtube.com/watch?v=ec8XEIjL2k8>

<https://www.youtube.com/watch?v=9AxovKzsrUI>

References, Article Source & Contributors

Cone, M. (2011, Dec. 17). *How to Configure Your Mac's Firewall*. Onttrek Oct. 24, 2015 uit MACINSTRUCT: <http://www.macinstruct.com/node/165>

Email tips. (s.j.). Onttrek Oct. 29, 2015 uit Digital Survival: <https://survival.tacticaltech.org/internet/email/tips>

How do I know if a website is secure? (2015, Oct.). Onttrek Oct. 29, 2015 uit ccm.net: <http://ccm.net/faq/2-how-do-i-know-if-a-website-is-secure>

How to Choose an Internet Browser. (s.j.). Onttrek Oct. 29, 2015 uit WikiHow: <http://www.wikihow.com/Choose-an-Internet-Browser>

How to Clear Your Browser's Cache. (s.j.). Onttrek Oct. 29, 2015 uit WikiHow: <http://www.wikihow.com/Clear-Your-Browser%27s-Cache>

How to Set up 2 Step Verification in Gmail. (s.j.). Onttrek Oct. 24, 2015 uit WikiHow: <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail>

How to Set up 2 Step Verification in Gmail. (s.j.). Onttrek Oct. 29, 2015 uit <http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail>

Lucas, I. (2009, July 10). *Password Guidelines*. Onttrek Oct. 24, 2015 uit Lockdown.co.uk: http://www.lockdown.co.uk/?pg=password_guide

Networking in Windows 7. (s.j.). Onttrek Oct. 24, 2015 uit <http://www.utilizewindows.com/>: <http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-in-windows-7>

NK, V. (2015, Jan. 24). *A Peek into the Top Password Managers*. Onttrek Oct. 24, 2015 uit opensourceforu.com: <http://opensourceforu.efytimes.com/2015/01/peek-top-password-managers/>

PROTECT THE SENSITIVE FILES ON YOUR COMPUTER. (s.j.). Onttrek Oct. 29, 2015 uit SECURITY IN-A-BOX: <https://securityinabox.org/en/guide/secure-file-storage>

PROTECT YOURSELF AND YOUR DATA WHEN USING SOCIAL NETWORKING SITES. (s.j.). Onttrek Oct. 29, 2015 uit securityinabox.org: <https://securityinabox.org/en/guide/social-networking>

Rusen, C. A. (2014, Sep. 09). *How to start & use the Windows firewall with advance security*. Onttrek Oct. 24, 2015 uit DigitalCitizen: <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security>

Rusen, C. A. (2014, Sep. 26). *How to Start & Use The Windows Firewall with Advanced Security*. Onttrek Oct. 29, 2015 uit <http://www.digitalcitizen.lif>: <http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advanced-security>

Talukder, M. i. (s.j.). *Free Antivirus*. Onttrek Oct. 29, 2015 uit http://shaifulaueo.blogspot.in/p/free-antivirus_13.html

The Home Computer Security Centre. (2009, july 10). Onttrek Oct. 29, 2015 uit <http://www.lockdown.co.uk>: http://www.lockdown.co.uk/?pg=password_guide

Tips for buying online. (2015, Oct. 02). Onttrek Oct. 29, 2015 uit Tips for buying online: <https://www.qld.gov.au/law/your-rights/consumer-rights-complaints-and-scams/consumer-advice-rights-and-responsibilities/tips-to-become-a-smarter-shopper/tips-for-buying-online/>

USE MOBILE PHONES AS SECURELY AS POSSIBLE. (s.j.). Onttrek Oct. 29, 2015 uit <https://securityinabox.org/en/guide/smartphones>

USE SMARTPHONES AS SECURELY AS POSSIBLE. (s.j.). Onttrek Oct. 29, 2015 uit <https://securityinabox.org/en/guide/smartphones>

What Is A Software Patch? (2013, Nov. 08). Onttrek oct. 29, 2015 uit OSSWATCH: <http://oss-watch.ac.uk/resources/softwarepatch>

Working With Windows Firewall in Windows 7. (s.j.). Onttrek Oct. 29, 2015 uit <http://www.utilizewindows.com>: <http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-in-windows-7>