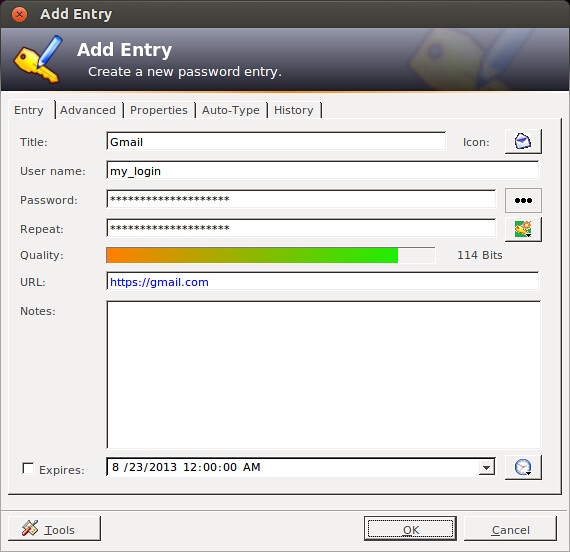
## **Some popular Password managers**

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.

### **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 customize 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.



#### **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.

### **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.

Graphical user interface, application

Description automatically generated

**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.

## **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.

Graphical user interface, application

Description automatically generated with medium confidence

**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: I**t 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.

### **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 favorites, 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.

Graphical user interface, application

Description automatically generated

**Gpassword manager**

#### **Features**

* **Access to favorite sites:**A list of favorite 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:** Favorite websites can be launched by right-clicking the tray icon.

### **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.

Graphical user interface, application

Description automatically generated

**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.

# WI-FI SECURITY

Internet users are widely using Wi-Fi devices to access Internet. Every year millions of Wi-Fi devices are sold in the market. Out of these most of the wireless devices are vulnerable in their default configuration mode. Since end users are not fully aware of security levels to be set on these devices, these get rendered vulnerable. By taking advantage of these unsecured Wi-Fi devices terrorists and hackers fulfill their needs.

Anyone with Wi-Fi connectivity in his computer, laptop or mobile can connect to unsecured Access Points(wireless routers).Anyone in the range of Access point can connect to an Access Point if it is unsecured. Once the connection is established the attacker can send mails, download classified/confidential stuff, initiate attack on other computers in the network, send malicious code to others, install a Trojan or botnet on the victims computer to get long term control on it through Internet, etc.

All these criminal acts will naturally be associated with the legal user of Access Point(wireless router). It is up to the legal user of the Access Point to defend himself to prove that he has not been involved in these acts. It now becomes the responsibility of the  user to secure his/her own Access Point.

Lets see some real incidents that took place in the recent years.

* Terrorists and hackers used unsecured Access Points to perform illegal activities on the Internet.
* Hackers penetrated into open Wi-Fi network of luxury hotels owned by the Thompson Group in New York, Los Angeles and Washington DC and stole the private emails sent by the guests.The hackers then attempted to extort money from the hotel chain by threatening to publish the emails.(www.crpcc.in)
* Just 5 minutes before Delhi blasts on September 2008 terrorists used an unsecured Wi-Fi connection of a company at Chembur in Mumbai to send terror emails to authorities and news channels. These hackers do not leave a trail of footprints for the investigators to arrive at a logical conclusion. The audit trail ends at Wi-Fi Access Point of the legal user. So it is becomes imperative for the users to secure their own Access Points(wireless router).

## **Types of Attacks on Wireless Environment**

### **Denial of Service Attack  Denial of service attack aims at preventing the users from accessing the network resources. In a Wireless network, denial of service attack can be applied in various ways.**

### **Man-In-Middle Attack in Wifi Devices**

Performing Man-In-Middle Attack in a wireless network is much easier, when compared to wired network. As the transmissons from an accesspoint is broadcasted, it is easy for an unauthorised user to collect the traffic sent by other wireless clients. And the process of collecting the packets in this manner is known as Eavesdropping. Also the third party user can manipulate the packets sent to the legitimate users which results in breaking the users privacy.

So In order to avoid these kind of attacks, Strong encryption should be used for transmitting the data between wireless client and accesspoint.

### **WarDriving**

It is a process of tracking Wi-Fi hotspots located at a particular place, while moving with a hand held device or a laptop in a vehicle. This helps the user in finding out the accesspoints that doesnot use encryption and takes control over it for performing the attacks on the network

#### **Tips:**

* All Wi-Fi equipment support some form of encryption. So, enable them.
* Enable MAC address filtering on Wi-Fi devices.
* Avoid dynamic IP address for home Wi-Fi rather use static IP addresses.
* Use encryption technology for sensitive data in wireless networks.

## **Guidelines for securing Wireless Communications**

* Always use strong password for encryption
* A strong password should have atleast 15 characters, uppercase letters, lowercase letters, numbers and symbol. Also it is recommended to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key. Do not use WEP for encryption, rather use WPA/WPA2.
* Always use the maximum key size supported by accesspoint for encryption
* If the keysize is large enough, then it takes more time to crack the key by the hacker. Also it is recommneded to change the encryption key frequently so that it makes difficult for the cracker to break the encryption key.
* Isolate the wireless network from wired network with a firewall and a antivirus gateway.
* Do not connect the accesspoint directly to the wired network. As there is a chance of comprimised wireless client inturn effecting the systems in the wired network, a firewall  and an antivirus gateway should be placed between the accespoint and the wired network.
* Restrict access to the Access Point based on MAC address
* In order to allow authorized users to connect to the Access Point, wireless clients should be provided access based on MAC address.
* Change the default username and Password of the Access Point
* Most of the users do not change the default passwords while configuring the Access Point.But it is recommended to keep a strong password, as this default password information can be known from product manufacturers.
* Shutdown the Access Point when not in use
* Hackers try to brute force the password to break the keys, so it is good practice to turn off  the Access points during extended periods of Non-use
* Do not broadcast your network name
* SSID information is used to identify a Access Point in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorized users to connect to the network, the information should not be provided in public.
* Always maintain a updated firmware
* Updating the firmware of  accesspoint is recommended, as it will reduce the number of security loop holes in the accesspoint.
* Use VPN or IPSEC for protecting communication
* When the information flowing from wireless client to the wired network receiver is critical, then it is recommended to use VPN or IPSEC based communication so that the information is protected from sniffers in the network.
* Do not make the SSID information public
* SSID information is used to identify a accesspoint in the network and also the wireless clients connect to the network using this information. Hence, in order to allow authorised users to connect to the network, the information should not be provided in public.
* Disable DHCP service
* When the number of users accessing the Access Point is less, it is recommended to disable the DHCP service. As this may make the attackers easy to connect to the network once they get associated with the Access Point.

SECURING COMPUTER USING FREE ANTIVIRUS

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 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 fromVirus, 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

# Email security

# Using Email

Email is a fast and efficient way to communicate. It is very useful for sending messages to which you need a timely reply, it's a great way to keep people informed about developments and it also makes it easy for people in different geographical locations and time zones to discuss topics and issues. It can be used as a tool for planning, and for content creation. However, email is not ideal for more nuanced discussions, and because it is text-based it can be easy for the tone of comments to be misunderstood.

You can access an email account in two ways, either using an application dedicated to receiving, sending and managing your messages, such as Outlook Express or Thunderbird, or via your web-browser, using online services like Gmail, Yahoo Mail, or Hotmail. Before doing anything, you will need to open an account with an email provider (see below).

The main thing to remember about email is that all data travels on the internet in a readable format, so if someone intercepts your email along the way, they can read the content easily. You would be surprised by just how many people could view this content if they wanted to. The internet is a huge, worldwide network of computers, all directing traffic among themselves, so there are very many different people who have the opportunity to intercept a message in this way.

## **Email Security**

# Few of the webmail providers available offer SSL access to your email. Some of them give you a secure login to protect your password but the messages you send and receive are not secure. Some even insert the IP address of the computer you are using into all of the messages you send. Two providers which are worth considering are Gmail and Riseup.

1. **GMAIL:**can be used entirely through a secure connection, as long as you login to your account from https://mail.google.com (with the HTTPS), rather than http://mail.google.com. To ensure ultimate security, you also need to set a preference that tells Gmail always to use SSL in sending and receiving mail. However, we don't recommend relying entirely on Google for the confidentiality of your sensitive email communication. Google scans and records the content of its users' messages for a wide variety of purposes and has, in the past, conceded to the demands of governments that restrict digital freedom.
2. **RISEUP:**If you don't have an email account yet, or wouldn't mind switching, the best we can recommend is Riseup https://mail.riseup.net. RiseUp offers free email to activists around the world and takes great care to protect the information stored on their servers. They have long been a trusted resource for those in need of secure email solutions. Unlike Google, they have very strict policies regarding their users' privacy, and no commercial interests that might conflict with those policies. In order to create a new RiseUp account, however, you will need two 'invite codes' which can be given out by anyone who already has a RiseUp account.

Regardless of what secure email tools you decide to use, keep in mind that every message has a sender and one or more recipients. Even if you are accessing your email account securely, your recipients may not be using a secure email account when reading and replying to your messages. To ensure private communication, you and your contacts should all use secure email services. If you want to be certain that messages are not intercepted between your email server and a contact's email server, you might all choose to use accounts from the same provider. In this case, RiseUp is a good one to choose.

## **E-Mail Security Tips**

* 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.