Digital Security: Overview, Types, and Applications Explained

We live in a time when much of our lives, personal and professional, reside online. We do our banking, music purchases, bill paying, social planning, and even parts of our job, in the digital world. This increased reliance on the internet and digital networks brings risks along with the convenience it provides.

Online criminals, hackers, even just bored mischief-makers lurk in the shadows, waiting to rob you, commit fraud, steal your identity, or simply embarrass you. Therefore, digital information security is of paramount concern.

What is Digital Security?

Digital security is the collective term that describes the resources employed to protect your online identity, data, and other assets. These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices.

In other words, digital security is the process used to protect your online identity.

What's the Difference Between Digital Information Security and Cyber Security?

You may have heard the term "cyber security" bandied about. That's hardly surprising since illegally accessing someone's data, identity, or financial resources is called a "cybercrime," which in turn creates a need for cyber security.

Yet, there's a difference between digital security and cyber security. Digital security involves protecting your online presence (data, identity, assets). At the same time, cyber security covers more ground, protecting entire networks, computer systems, and other digital components, and the data stored within from unauthorized access.

You could make a case for calling digital security a sub-type of cyber security. Many industry professionals use the two terms interchangeably, but in reality, digital security protects information, and cyber security protects the infrastructure, all systems, networks, and information.

Why is Digital Data Security Important?

This infographic from 2019 shows some of the most significant data security breaches of the past decade. As if that wasn't alarming enough, this article reports that over seven million data records get compromised each day, and incidents of cyber fraud and abuse increased by 20 percent in the first quarter of 2020.

What is Digital Security: Overview, Types, and Applications Explained

Cybercriminals are opportunists attracted by the sheer volume, value, and variety of data available for exploitation. And all they need is just one good haul to make their efforts worth it. If they can fool only one consumer—through a phishing attack, for example—hackers could reap the rewards of a stolen identity or a compromised credit card with a substantial balance to burn through.

Like we said at the start, our increased reliance on the internet means we have a lot more to lose if something goes sideways. The stakes are raised; we need impeccable, reliable digital data security.

What Kind of Information is Considered a Digital Security Risk?

Not every bit (or byte) of your information is useful to cybercriminals. A total stranger finding out that you prefer the original Star Wars trilogy to the sequels is scarcely an earth-shattering revelation that could compromise your identity or financial security. So, what kinds of data are at risk?

- **Personal Identification Data**

  This data includes your name, phone number, address, email account name, IP address, and, most damaging, your Social Security number. It also includes information that potentially pinpoints your location. Personal data is often used for identity theft and social engineering. Also, a hacker who has your Social Security number (or equivalent) can open credit card accounts in your name, thereby eventually destroying your credit score.

- **Personal Payment Data**

  If it has to do with financial transactions, it's considered personal payment data. This information includes credit and debit card numbers (including expiration dates), online banking numbers (account and routing), and PIN codes. Criminals who gain access to your online banking information can even transfer funds out of the accounts or make purchases.

- **Personal Health Data**

  Also known as personal health information (PHI), this data type encompasses information on your health, including medical history, prescription drugs, health insurance subscriptions, and doctor and hospital visits. This information is precious to high-rolling cybercriminals since they can use your health information to file false insurance claims or order and resell prescription drugs.

What Are the Different Types of Digital Security?

As you can see, there is a lot that can go wrong if your digital data is compromised. Fortunately, security in the digital world comes in many forms, offering a wide choice of defense methods. These include:

- **Antivirus Software**

  Viruses delivered through malware and other malicious systems infect your data and bring your system to a screeching halt. A good antivirus program not only detects and cleans out these infections, but also keeps out suspicious programs and isolates likely threats.

- **Current, Updated Firewalls**

  This tool monitors web traffic, identifies authorized users, blocks unauthorized access, and—if current enough—will even protect against next-generation viruses. Firewalls have been around for years, and many cyber security experts dismiss them as obsolete. However, a state-of-the-art version is a potentially useful tool for keeping out unwanted users.

- **Proxies**

  Proxies are digital security tools that bridge the gap between users and the internet, using filtering rules in line with an organization's IT policies. Proxies block dangerous websites and leverage an authentication system that can control access and monitor usage.

- **Remote Monitoring Software**

  Remote monitoring allows the data security team to collect information, diagnose problems, and oversee all the applications and hardware from a remote location. Remote monitoring provides flexibility and convenience, enabling administrators to resolve any issue anytime, anywhere.

- **Vulnerability Scanner**

  This tool detects, evaluates, and manages any weak spots in your organization's system. Vulnerability scanners not only identify flaws but also prioritizes them to help you organize your countermeasures. IT security teams can use scanners for both web applications and internal systems.

What Are Some Specific Examples of Digital Security Tools?

We've discussed the various types of digital security, but now we're going to explore some specific security tools available. These tools protect the integrity of your information flowing back and forth between various online media since this is a particularly vulnerable (and often-used) target for criminals and hackers.

- **Instant Message Encryption Tools**

  You would be surprised how much sensitive information passes through IMs. ChatSecure is a messaging app that offers secure encryption for Android and iOS phones, and

  Cryph secures your Mac or Windows-based web browsers.

- **Navigation Privacy Tools**

  Criminals can't steal what they can't see. Anonymox protects your identity by creating a proxy, letting you change your IP and surf anonymously. It's available as an add-on for Google Chrome and Firefox. Tor isolates every website you explore, so advertisements and third-party trackers can't lock into you. It also clears your browsing history, removes cookies, and provides multi-layer encryption.

- **Telephone Encryption Tools**

  SilentPhone offers smartphone users end-to-end encryption for voice conversations, messaging, file transfer, video, and more. It's compatible with Android and iOS devices and is free. Signal is an independent nonprofit resource that lets users share text, GIFs, voice messages, photos, videos, and data files.

What is DHCP and why it is used?

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway

Configuring Firewall on MAC system

How to Configure Your Mac's Firewall

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.

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.

Turning on and Configuring the Mac OS X Firewall

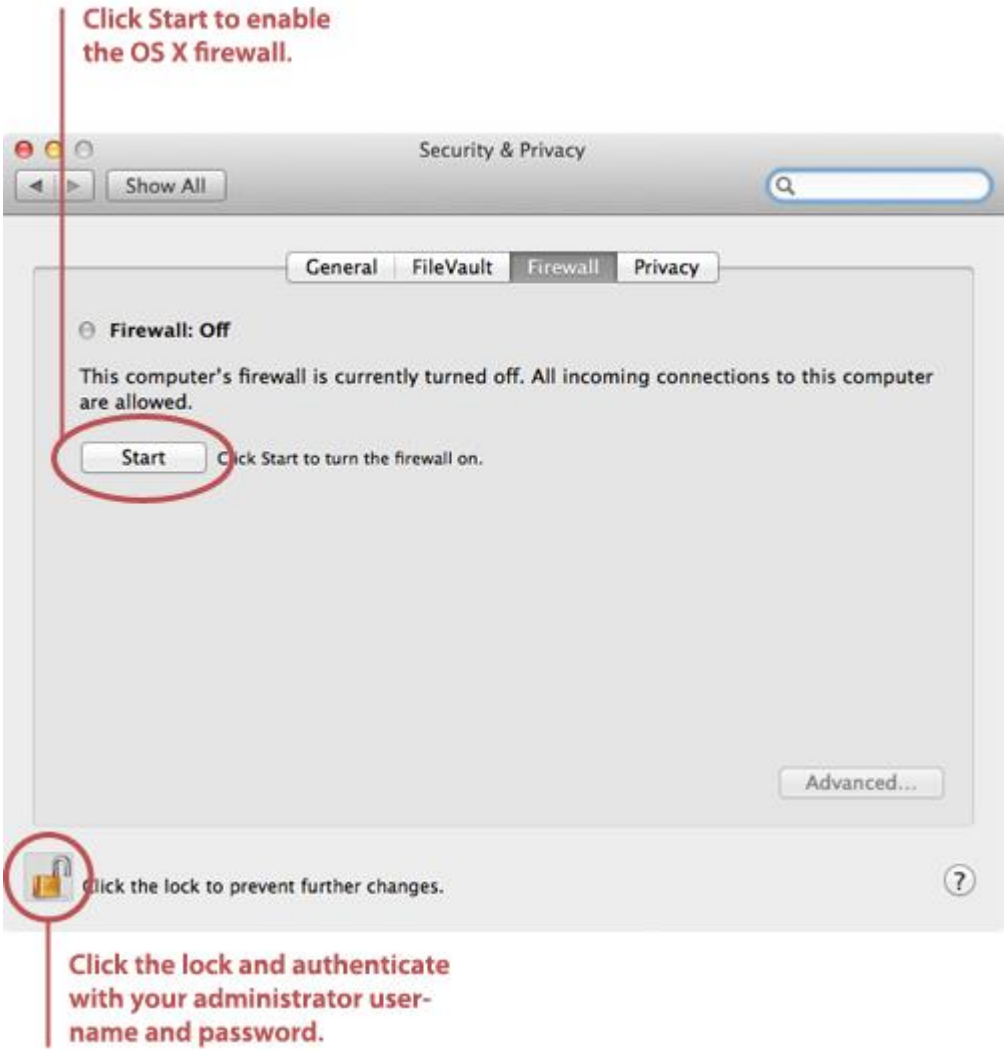
Here's how to turn on and configure your Mac's built-in firewall:

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

2. Select **Security & Privacy**.

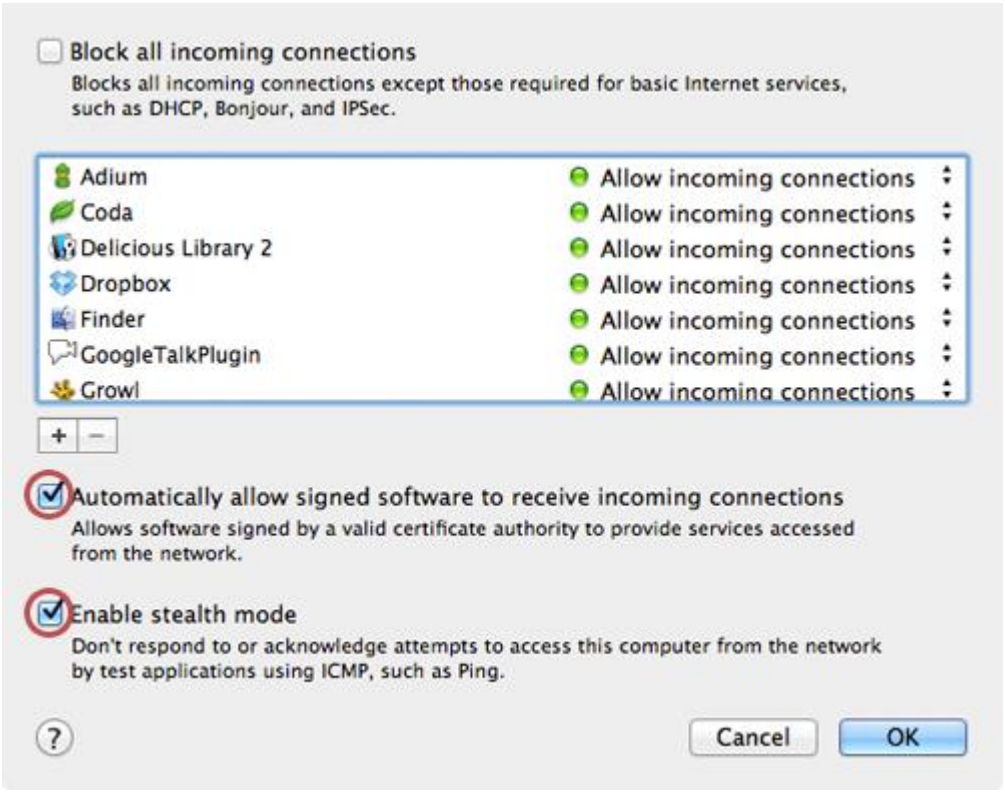
3. Click the **Firewall** tab.

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!

What is the Windows Firewall and how to turn it on or off?

Windows Firewall

The Windows Firewall is a silent tool that keeps our systems safe from all kinds of network threats and has been included in each version of Windows for the last decade. Because it is a silent ally, doing most of its work in the background, few users interact with it on a regular basis, and even fewer know what this tool is and how it works. That's why, in this article, we will explain what the Windows Firewall is, what it does, how to find it and how to enable it or disable it, depending on whether you want to use it or not. Let's get started:

What is the Windows Firewall?

The Windows Firewall is a security application created by Microsoft and built into Windows, designed to filter network data transmissions to and from your Windows system and block harmful communications and/or the programs that are initiating them. Windows Firewall was first included in Windows XP (back in 2001), and since then it has been improved in each new version of Windows. Before 2004 it used to be named Internet Connection Firewall and, at that time, it was a rather basic and buggy firewall with lots of compatibility issues. Windows XP Service Pack 2 changed its name to Windows Firewall and introduced and improved core capabilities such as that of filtering and blocking incoming connections.

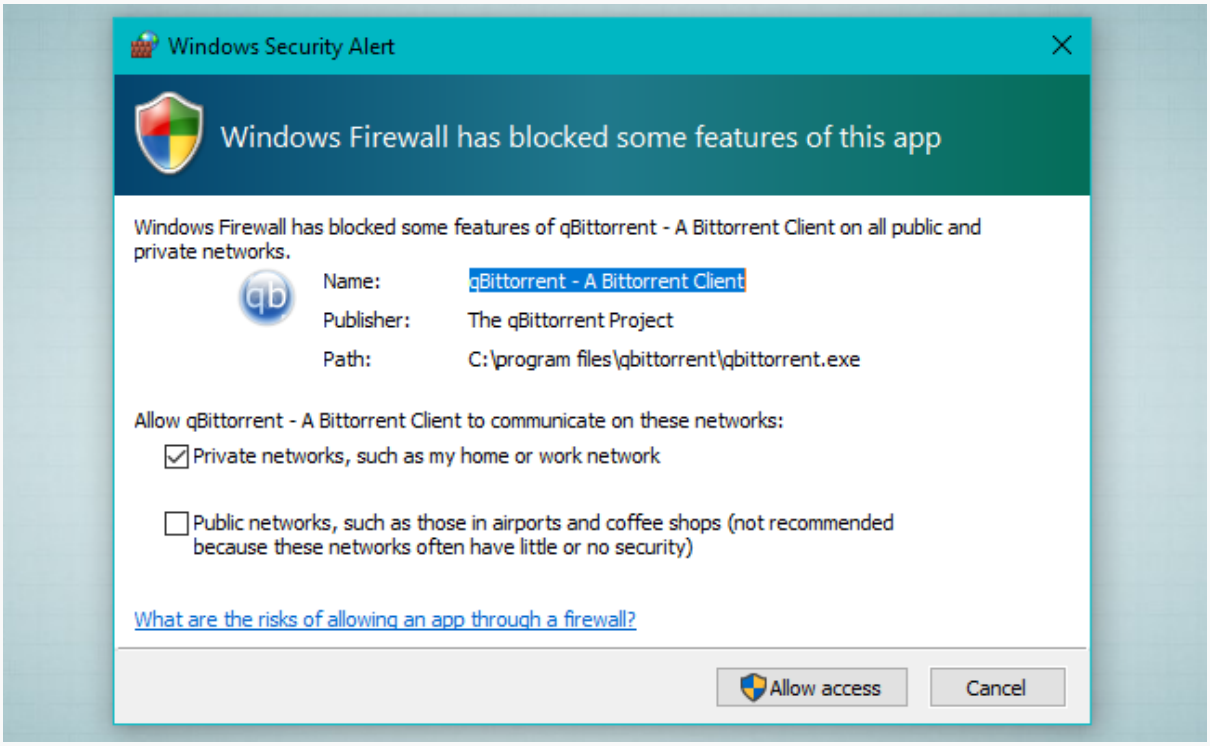
What does the Windows Firewall do for you?

Windows Firewall can provide your computer or device with protection against attacks from your local network or the internet, while still giving you access to the network and the internet. Because Windows Firewall filters the traffic that goes on your computer, it can also stop types of malicious software that use network traffic to spread themselves, like Trojan horse attacks and worms. Another useful capability is that it can filter both outgoing and incoming connections to your Windows computer and block those which are unwanted. The firewall uses a predefined set of rules for both types of network traffic, but its rules can be edited and changed both by the user and the software that the user installs.

By default, the Windows Firewall lets you do many things such as browsing the internet, using instant messaging apps, connecting to the Homegroup on your local network, sharing files, folders and devices, and so on. The rules are applied differently depending on the network profile set for the active network

connection. If you are not familiar with this concept, we recommend you to read this article: Simple questions: What are network locations in Windows?.

Most Windows programs that need internet and network access, automatically add their exceptions to the Windows Firewall, so that they can work correctly. If they don't add such an exception, the Windows Firewall displays a Windows Security Alert, in which they ask you to allow them access to the network. You can see an example in the screenshot below.



By default, the Windows Firewall selects the checkbox that is appropriate for the network connection that you are using. You can select either of the options or both, depending on what you want to do. If you want to allow a program to connect to the network and the internet, click or tap Allow Access. If you want to block access, press Cancel.

If you are using Windows with a user account that is not an administrator, you will not see such prompts. All programs and apps are filtered according to the rules that exist in the Windows Firewall. If an application doesn't comply with this regulation, it is automatically blocked, without any prompts being displayed. Windows Firewall is turned on by default in modern Windows versions such as Windows 10, Windows 7 and Windows 8.1, and it runs silently in the background as a service. It only prompts users when they need to make a decision. You won't have to open it unless you want to see its status or configure the way it works.

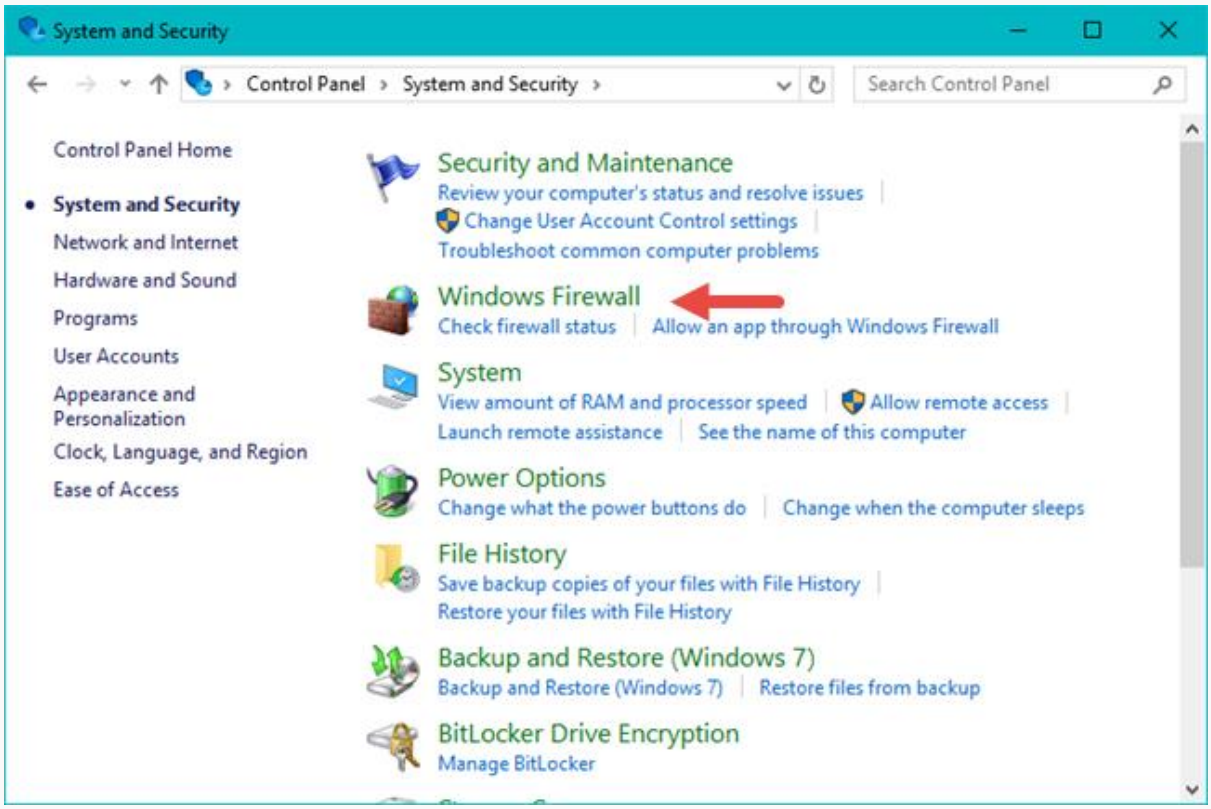
What doesn't the Windows Firewall do?

The Windows Firewall cannot protect you against any malicious attacks. It is a tool that should always be used in conjunction with a good antivirus program because it acts as a barrier between your computer and the outside world. It cannot protect your Windows computer from malware that's already present on it. If it happens that your computer is infected with spyware or a ransomware, then Windows Firewall is not going

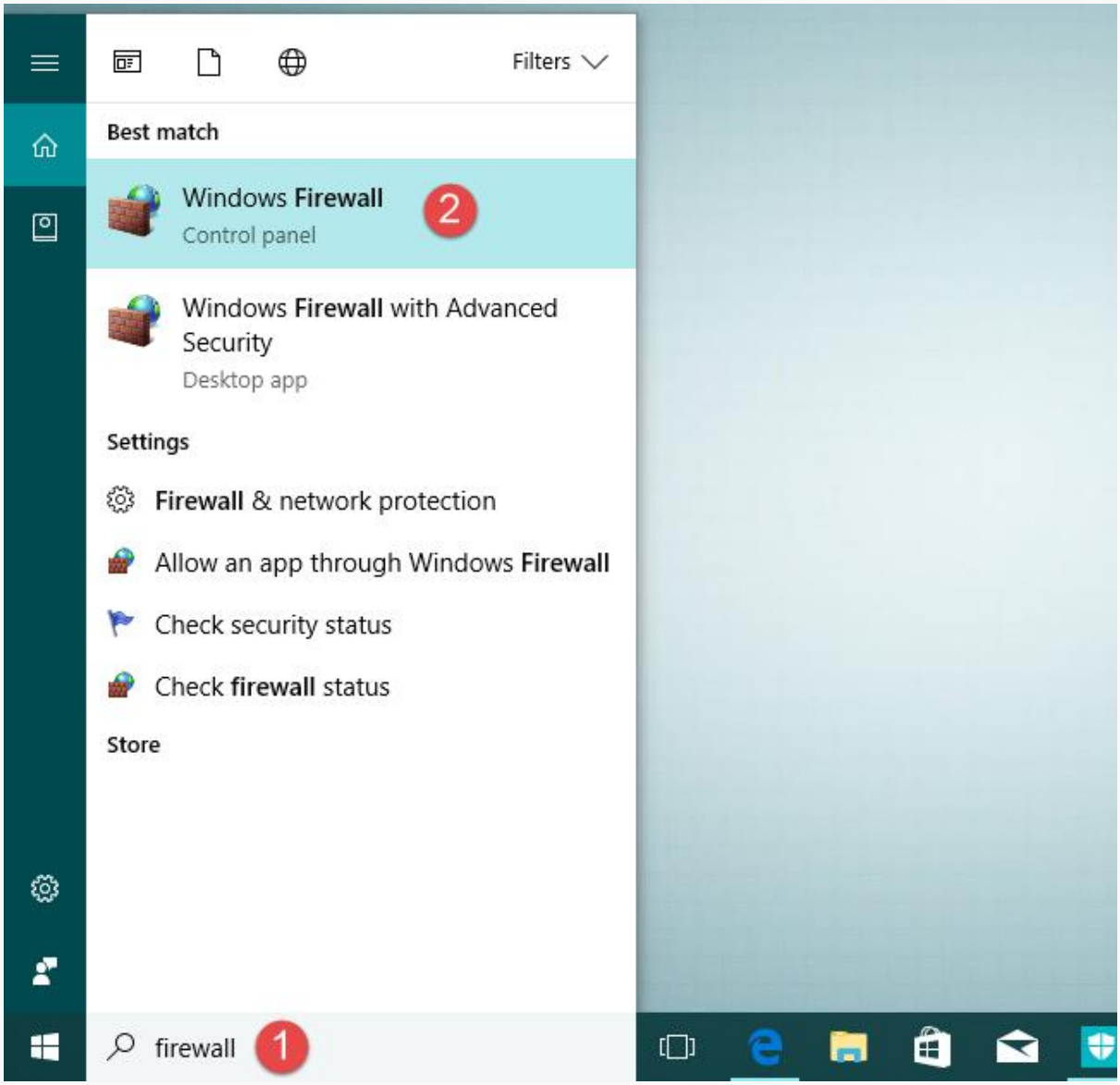
to be able to stop the communications between the malicious code and the remote hackers. You would need a third-party tool for this task, like Heimdal Pro.

Where to find the Windows Firewall

To open the Windows Firewall, you have several options. One of them is to go to "Control Panel -> System and Security -> Windows Firewall." This applies to both Windows Windows 10, Windows 7, and Windows 8.1.



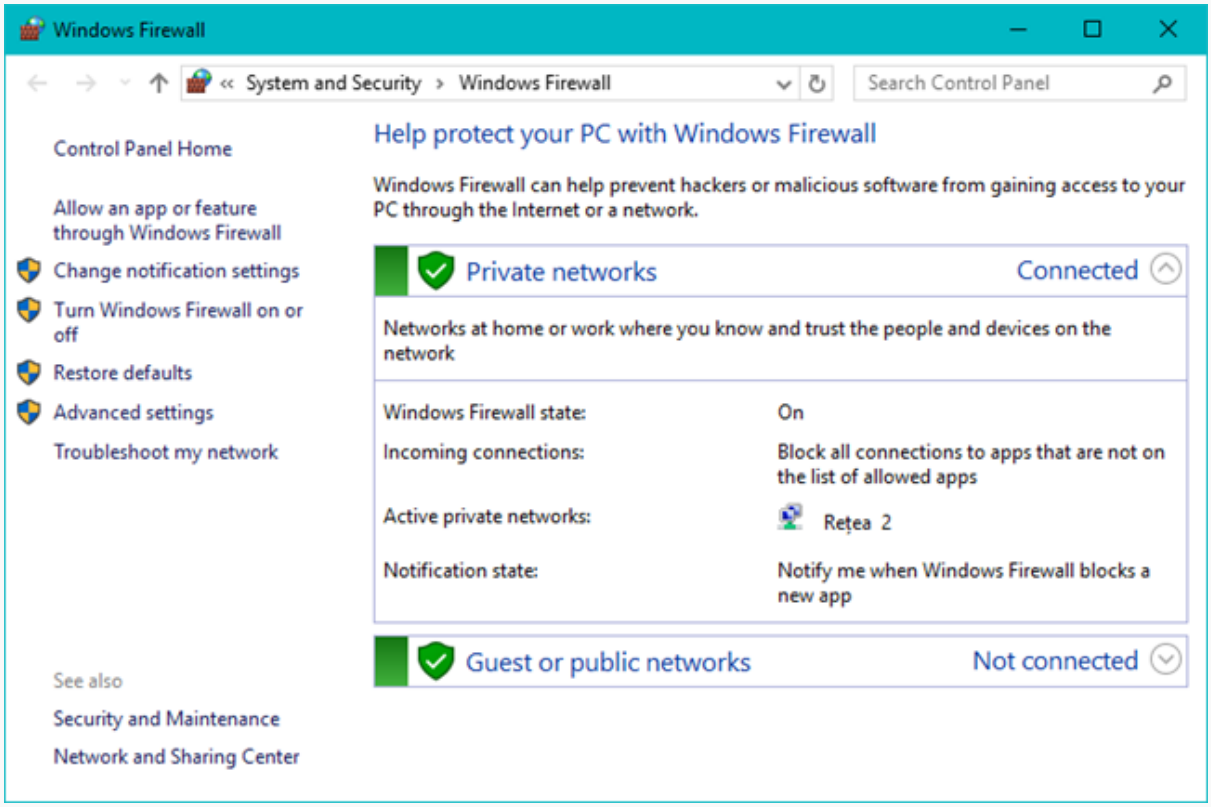
In Windows 10, you can use Cortana by asking her to search for "firewall." Once she has the answer, you can click or tap on the Windows Firewall search result.



In Windows 7, you can use the Start Menu search box and type the word firewall. Click on the Windows Firewall search result shown below.

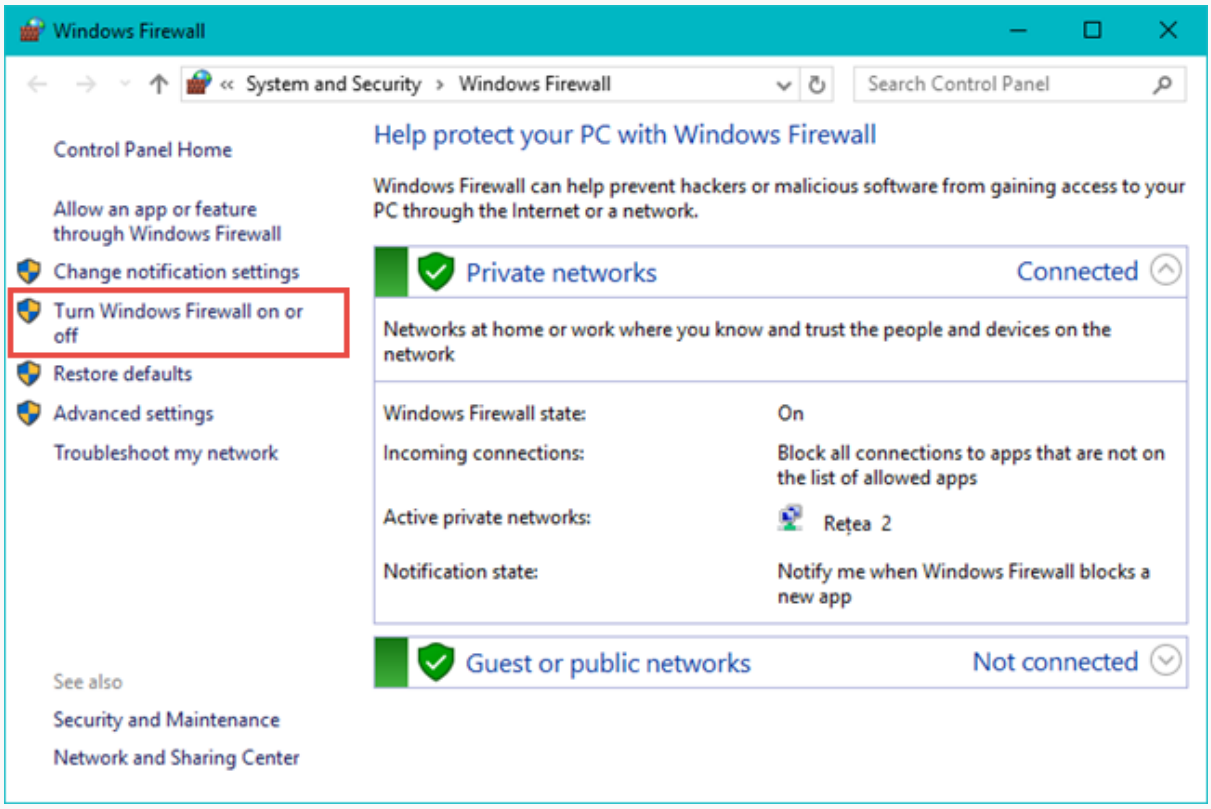
In Windows 8.1, go to the Start screen and type the word firewall. Then, click or tap the Windows Firewall search result.

When you open it, you will see a window similar to the one below: showing the type of network you are connected to and whether the firewall is turned on or off.

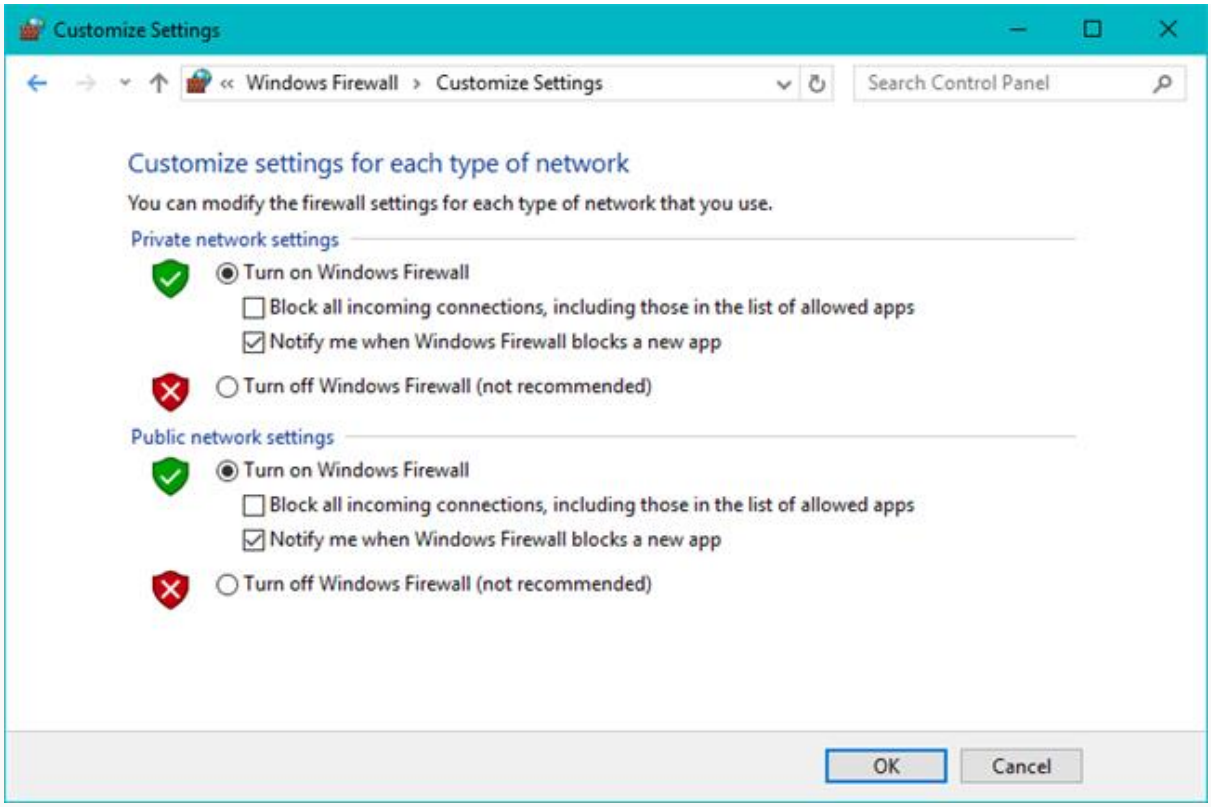


How to turn the Windows Firewall on

To activate or deactivate the Windows Firewall, click or tap the "Turn Windows Firewall on or off" link, found on the left side of the Windows Firewall window.

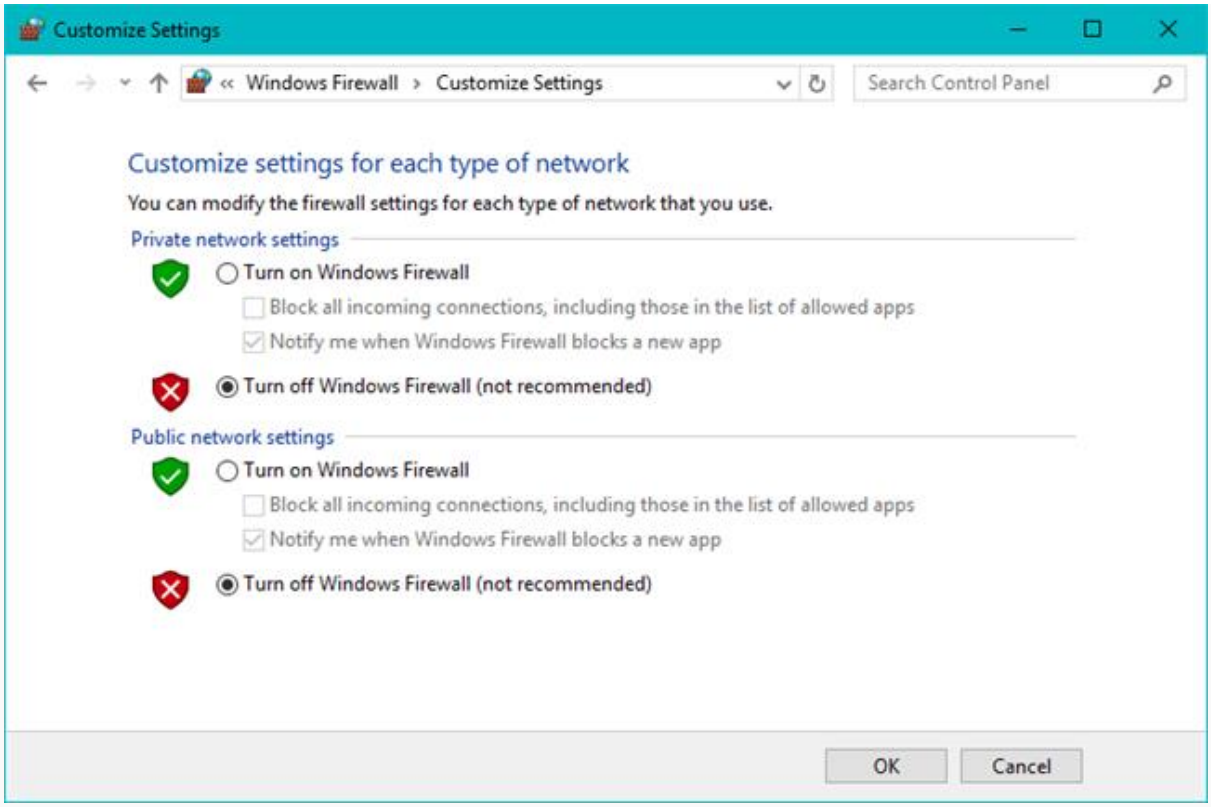


By default, the Windows Firewall is turned on for both types of network locations: private (home or work in Windows 7) and public. If you want to turn it on or off for any of these network locations, check the appropriate "Turn on/off Windows Firewall" box and press OK.



How to turn the Windows Firewall off

To disable Windows Firewall, you need to select "Turn off Windows Firewall" for both types of networks and press OK.



On a final note, please keep in mind that you can turn the Windows Firewall on or off only if you are an administrator. Your setting applies to all the user accounts that exist on your Windows device. Also, if you choose to disable the Windows Firewall make sure that you have a reliable alternative installed, like a third-party firewall or internet security suite.

INTRODUCTION TO MOBILE PHONES

Smartphones are one of the most empowering technologies to which most people in the world have access. At the same time, they are bristling with sensors, nearly always within arms reach and usually connected to some network or another. In short, they face most of the security challenges we associate with computers, plus a number of additional threats related to portability, ubiquity, insecure network architecture, location tracking, media capture and other such considerations.

OPERATING SYSTEMS

Most smartphones run one of two operating systems: Google's Android or Apple's iOS. Android devices are sold by many different companies. Their software is often modified by their manufacturers and by service providers who hope — and sometimes require — that their owners will rely on (and pay for) access to their mobile phone networks. iOS works only on Apple devices and makes it much more difficult to run applications that have not been approved by Apple.

The reliability of operating system updates is one of the most important considerations when buying an Android smartphone. Some cheaper models do not provide access to updates that are needed to fix important security flaws. This could leave you vulnerable to malware or other attacks.

BRANDED AND LOCKED SMARTPHONES

Smartphones are often sold locked to a specific carrier or mobile network operator. This means that the specific smart phone will only work with that company's SIM card. Mobile network operators often customise the operating system and install additional software on locked smartphones. They may also disable some functionality. This could leave you with apps on your smartphone that you cannot uninstall or prevent from accessing your information, including your contacts and storage.

For these reasons, it is usually safer to buy an unlocked smartphone that is not locked to a particular mobile provider. Unfortunately, these are often more expensive.

BASIC SECURITY SETUP

Smartphones have a number of settings that can help you manage the security of the device. It is important to pay attention to how your smartphone is set up. The Tool Guide below suggests a few specific Android settings and applications:

INSTALLING, EVALUATING AND UPDATING APPLICATIONS

The easiest — and typically the safest — way to install new software on your smartphone is to use Google's Play store for Android or Apple's App Store for iOS devices. Sign in from your device and you can download and install applications.

You can find Android apps in various places online, but you should generally avoid installing them. Some of these apps contain malware. You can learn more about malware in the Tactics Guide on how to Protect your device from malware and phishing attacks. Only install software that comes from a source you trust. And keep in mind that trusted individuals may inadvertently spread malware without realising it. Applications in the Play Store and in the App Store benefit from a limited review by Google and Apple, respectively. This provides some protection against overtly malicious software.

For experienced Android users, and for those who are unable or unwilling to rely on Google's Play Store, **F-Droid** is one possible exception to this rule. It is an alternative app center that only distributes FOSS applications. If you need access to F-Droid, you can install it from a trusted source and then use it to install other apps. You can also install Android Application Packages (.apk files) directly if you enable your device's Install Unknown Apps setting. Again, this is risky, but if you have no other way to install an application you need, you can have someone you trust give you the .apk file on a flash memory card.

Even "official" apps sometimes behave poorly. On Android devices, each application must ask your permission before it will be permitted to do certain things. You should pay close attention to what permissions are requested. If they do not make sense for the app in question, have a look at the reasons provided and consider declining and uninstalling the app. If you are testing out a "news reader" app, for example, and it asks for permission to send your contacts over a mobile data connection to a third party, you should be suspicious. (Some app developers collect lists of contacts and sell them or use them for marketing.)

Remember to keep all of your apps up-to-date and to uninstall apps that you no longer use. App developers sometimes sell their apps to other people. A new owner could alter an app that you have already installed and push a malicious update.

MOBILITY AND THE VULNERABILITY OF INFORMATION

The mobile phones we carry around with us often contain sensitive information. Call logs, browser histories, text and voice messages, address books, calendars, photos and other useful functions can become liabilities if the device on which they are stored is lost or stolen. It is important to be aware of the sensitive information on your mobile phone as well as the online data to which it grants automatic access. These data have the potential to endanger not only the device's owner, but everyone who appears in their address book, inbox or photo album.

Once you have thought through the possible risks and familiarised yourself with the privacy and security features supported by your device, you can start putting safeguards in place.

STORING INFORMATION ON YOUR SMARTPHONE

Modern smartphones have a lot of room to store data. Depending on the device, however, it may be quite easy for anyone with physical access to extract that information.

DEVICE AND DATA ENCRYPTION

Recent iOS devices have strong encryption turned on by default, as long as you set a strong passcode. Android supports device encryption as well, and you should enable it if you can. Remember to back up the contents of your smartphone before turning on full disc encryption in case there is a problem while the phone is encrypting itself.

Android also allows you to encrypt the data on any flash memory cards (such as MicroSD cards) if you use them.

When you turn on an encrypted phone and enter your passcode, it allows you to access and modify the content on it. This means that someone with physical access to your encrypted smartphone, while it is powered on and unlocked, can still access your data. For the strongest protection — when crossing a border, for example, or passing through airport security — you should turn your device off completely.

As usual, there are trade-offs. If you believe you might need the ability to make an emergency call on short notice, for example, it might be worth taking the risk of leaving your phone powered on and just locking the screen.

If you are not able to activate full disk encryption, or if you need extra security for particular files, you might want to install a few additional Android tools. Some apps encrypt their own data, and the OpenKeychain app allows you to encrypt other files. If you use it alongside K-9 Mail, you can also send and receive encrypted email. (There is no free equivalent to these tools on iOS.) Apps like these can help you protect your sensitive data, but you should still enable device encryption if possible.

It is also important to minimising the amount of sensitive information you store on your device, especially if device encryption is not an option. Some phones have the ability to disable the logging of phone calls and SMS text messages, for example. You could also adopt a policy of deleting sensitive entries from your call and message history.

RECORDING PASSWORDS SAFELY

You can store most of your passphrases in a single, encrypted file on an Android device by installing a FOSS tool called KeePassDroid. This app allow you to remember a single, strong master passphrase and use it to lookup your other passphrases. This, in turn, makes it possible to choose strong, unique passphrases, for all of your accounts, without having to memorise them. KeePassDroid also provides a random password generator you can use when creating new accounts.

If you use KeePassXC or KeePassX on your computer, as discussed in our Tool Guide on how to Create and maintain secure passwords, you can copy your encrypted (.kdbx) database file onto your mobile device.

There is a similar tool for iOS devices called MiniKeePass.

BEST PRACTICES FOR PHYSICAL PHONE SECURITY

Restricting physical access to your mobile phone is the first line of defence for the information it contains. You should keep it on you at all times, except where doing so presents a specific security risk. This applies to SIM cards and flash memory cards, as well. Even if you are concerned about malware or advanced surveillance, it may be safer to remove the battery and keep the device with you rather than leaving it unattended.

In addition to turning on encryption and keeping your phone nearby, below are a some additional steps you can take to maintain the physical security of your mobile device and limit the damage if it is lost or stolen.

GENERAL STEPS

- Always set a strong screen lock code and avoid sharing it with others. If you are using a basic phone that came with a default lock code, change it.
- Avoid storing sensitive information, including phone numbers, on a SIM card, as they cannot be encrypted.
- Regularly backup important data from your phone on your computer or on an external storage device. Store these backups securely as described in How to protect the sensitive files on your computer. Having a backup will help you remember what information is on your phone and make it easier for you to restore it to its factory settings in an emergency.
- Phone numbers are often linked to important accounts, and it is sometimes possible for an attacker to take over your phone number to gain access to those accounts or to impersonate you. Some mobile network providers allow you to set a PIN or password on your account to prevent unauthorised people from making changes to your account or stealing your phone number. You should take advantage of this feature if it is available.
- If you are concerned about malware, consider placing a small, removable sticker over your phone's cameras.

STEPS RELATED TO LOSS AND THEFT

Mobile phones have a 15-digit International Mobile Equipment Identity (IMEI) number that helps identify them on mobile networks. Changing SIM cards does not change your IMEI. This number is often printed behind the battery, and most phones will display it in their Settings or if you dial *#06#. Make a note of this number, as it could help you prove that you are the owner if your phone is stolen.

Consider the advantages and disadvantages of registering your phone with your service provider. If you report a registered phone stolen, your service provider can usually disable it. However, registering your phone may associate it more strongly with your actual identity.

Most Android phones and iPhones have a built-in anti-theft or "Find my Phone" feature that allows you to track or disable your phone if it is stolen. There are also third party tools that do the same thing. These tools involve trade-offs, but if you trust those who operate the service (and the quality of their software), you might want to enable one and practice using it.

STEPS TO TAKE WHEN GIVING YOUR DEVICE TO SOMEONE ELSE

When disposing of, giving away or selling a phone, make sure you do not also hand over the information stored on its SIM card or on a flash memory card. These storage devices may contain information even if they are expired or no longer working. Dispose of SIM cards by physically destroying them. Remove and keep (or destroy) flash memory cards. The best way to protect data on the phone itself is make sure it is encrypted and then reset the device to its "factory settings."

Try to use trusted phone dealers and repair shops. This reduces the vulnerability of your information when getting second-hand hand phones or having your phone repaired. If you think someone might have the access, resources or motivation to target you by pre-installing malware on your device before you buy it, consider choosing an authorised phone dealer at random.

Remove your SIM card and flash memory cards if you take your phone to a repair shop to be serviced.

MOBILE INFRASTRUCTURE, TRACKING, SURVEILLANCE AND EAVESDROPPING

Mobile phones and mobile phone networks are inherently less secure than we tend to realise. In order to send and receive calls and messages, your phone is constantly communicating with the nearest cell towers. As a result, your service provider knows — and keeps a record of — your phone's location whenever it is powered on.

ABOUT THE INTERCEPTION OF PHONE CALLS AND TEXT MESSAGES

Mobile networks are typically private networks run by commercial entities. Sometimes your service provider owns the mobile network infrastructure and sometimes it resells mobile service that it rents from another company. SMS text messages are sent unencrypted, and phone calls are either unencrypted or weakly encrypted. Neither are encrypted in a way that would protect them from the

network itself. As a result, both your service provider and the owner of the cell towers you are using have unlimited access to your calls, text messages and location. In many cases, the local government has the same access, even in places where it does not own the infrastructure itself.

Many countries have laws or policies that requires service providers to maintain a long-term record of all SMS text messages sent by their customers. And most service providers keep such logs anyway, for business, accounting or dispute resolution purposes. Similar regulations exist for call records in some places.

Furthermore, the operating systems that run on mobile phones are often built or modified to the specification of one or more service providers. As a result, the operating system itself may include hidden features that make this kind of monitoring even more invasive. This applies to basic mobile phones and smartphones alike.

In some cases, voice and text communication can also be intercepted by a third party. If an attacker is able to place an inexpensive piece of equipment — an IMSI catcher — within range of a target's mobile phone, they can fool it into communicating with that device as if it were a legitimate cell tower. (IMSI catchers are sometimes referred to as Stingrays, which is a well known brand name under which they are marketed to law enforcement.) In a few known cases, third party attackers were even able to gain access to mobile networks from across the globe by exploiting vulnerabilities in Signalling System Number 7 (SS7), which is an international exchange for voice calls and SMS text messages.

Finally, even when connecting through WiFi rather than using a mobile network, smartphone and tablet operating systems are designed to encourage the sharing of personal data through social networking platforms, cloud storage services, aggressive use of the global positioning system (GPS) and other such features. While many people enjoy this aspect of Android and iOS, it can easily lead to the exposure of sensitive information.

When thinking about how to protect your sensitive communications, you can start by asking yourself a few questions:

- With whom do you communicate, when and how often?
- Who might be interested in the fact that you are speaking with this person?
- How confident are you that the other party is who they claim to be?
- What is the content of your calls and messages?
- Who might be interested in that content?
- Where are you calling from, and where is the other party?

If the answer to these questions gives you cause for concern, you should think about how to minimise the associated risks. To do so, you might have to help the other party adopt a new tool or technique. And, in some cases, you might have to avoid using a mobile phone when communicating with them.

ABOUT ANONYMITY

Protecting the content of your calls and messages can sometimes be challenging, but remaining "anonymous" when using a mobile phone is even more difficult. In particular, it is rarely possible to hide the fact that you are communicating with a given individual when placing a call or sending an SMS text message. Using a secure messaging app through a mobile data or WiFi connection can help, but there are no guarantees for this kind of thing. Often, the closest you can get is to choose

which third party has access to this information and hope that they are unlikely to cooperate with those from whom you are trying to hide your communication.

In order to achieve a greater level of anonymity, people sometimes choose to use disposable phones and short lived accounts. This technique remains effective in some situations but is far more difficult to pull off than it might seem. The simplest approach is for both parties to buy basic, pre-paid phones and use them to make calls and send SMS text messages for a very limited period of time before disposing of them. There is no way for them to encrypt their communication, however, and the effectiveness of this technique rests on quite a long list of assumptions. That list includes, at a minimum:

- That both parties purchase phones and SIM cards with cash,
- That they are not observed or tracked via their real phones while doing so,
- That they can activate their SIM cards without showing identification to register them,
- That they remove the batteries from their phones when they are not in use,
- That they are able to exchange phone numbers without being observed,
- That they use their phones in locations where they do not usually spend time,
- That they leave their smartphones elsewhere while doing so, and
- That voice recognition technology is not more advanced than we think.

Managing all of this for a pre-paid smartphone would make it possible to place encrypted voice calls and send encrypted messages while hiding the link between the two parties. Doing so effectively would demand even more care and attention, however, in part because smartphones and secure messaging apps require account registration. There is little value in using an "unlinkable" phone to access services that are already associated with your real identity. Creating anonymous email accounts and signing up for single-use online services can be quite time consuming and require additional knowledge and discipline. Both parties would need to understand how IP addresses work, what browser fingerprinting is and how to use the Tor Browser or Tails, among other things. They would have to spend more money and more time at random Internet cafes without their real phones.

ABOUT EAVESDROPPING

Phones can be set to store or transmit data from their microphones, video cameras and global positioning sensors without notifying the user. This is true of both basic mobile phones and smartphones. Malware is responsible for most such attacks, but service providers are also believed to have engaged in this kind of surveillance against devices connected to their network. Some phones can even be switched on remotely and used to spy on their owners while appearing to remain off.

Avoid giving people you do not trust physical access to your phone. This is often how malware ends up on mobile devices.

Don't forget that using a mobile phone in public, or in a location that you think might be monitored, leaves you vulnerable to traditional eavesdropping techniques. It may also put your phone at risk of being stolen.

Encourage those with whom you communicate about sensitive matters to adopt the same tools and tactics you deem appropriate for yourself.

If you are conducting a private, in-person meeting, switch your phone off and disconnect the battery. To avoid revealing the location of the meeting, it is best to do this before departing for that location. If you cannot remove your battery, leave your phone somewhere safe.

COMMUNICATING OVER THE INTERNET ON YOUR MOBILE PHONE

As discussed in our Tactics guides on how to keep your online communication private and on how to remain anonymous and bypass censorship on the Internet, sending information to and receiving data from the Internet can leave traces that identify who you are, where you are and what you are doing. Nevertheless, some Android and iOS tools that rely on the Internet to communicate are far safer than using the mobile network to place a voice call or send an SMS text message.

Smartphones allow you to control how you access the Internet. Typically, you can connect through WiFi or through a mobile data connection offered by your service provider. Using a WiFi connection may reduce the traces accessible to your service provider, but it reveals that same information to the operator of the wireless access point you are using and to their Internet service provider (ISP). In some countries, mobile service providers are subject to different regulations than internet service providers, which can result in different levels of surveillance by the relevant companies and by government agencies.

However you choose to connect your smartphone to the Internet, encryption and anonymity tools can help you protect the information you send and receive.

USING SECURE MESSAGING APPS

As mentioned above, phone calls and SMS text messages are quite insecure. Voice over IP (VoIP) is a way of making voice calls using an Internet connection rather than a mobile phone network. Text communication can also be sent over the Internet, and there are a number of modern messaging apps that use encryption to do both securely.

Signal is a FOSS app that encrypts individual and group text messages to and from other people who use Signal. It also offers encrypted voice and video calls between two Signal users. It is easy to install, easy to use and integrates itself with your existing list of contacts. Signal is available for both Android and iOS and can be used on a Windows, Mac or Linux computer, as well, once you have it running on a smartphone.

For the sake of simplicity, Signal uses your mobile phone number as a way to identify you to your contacts. Unfortunately, this makes it difficult to use Signal without a functioning mobile service plan, even on WiFi-enabled devices. This also means that you have to share your phone number with people you want to connect with over Signal. If those restrictions are problematic for you, there are a handful of other reputable secure messaging apps. Wire is one popular alternative (Android, iOS).

Below are some criteria that you might consider when choosing a mobile messenger app:

- What do digital security experts say about it?
- Is it Free and Open Source Software?
- Does it support end-to-end encryption one-on-one communication?
- Does it support end-to-end encrypted group text communication?
- Does it support end-to-end encrypted group voice communication?
- Are file transfers end-to-end encrypted?
- Can you set your messages to "self destruct?"
- Will it work over a low bandwidth network connection?
- Who are the developers, and do you trust them?
- Who operates the server and what information do they claim to store about your calls and messages?
- Does it work on
- Can you use the same account on multiple devices?
- Does it work on all major operating systems?
- Does it allow you to register with an email or a username, rather than an phone number, so that you can separate your contact information from your actual identity?
- Can you use it without giving it access to the list of contacts on your device?
- Can you use it on a mobile device that is not a phone?
- Can you or someone you trust run your own server and use it to communicate?

SENDING AND RECEIVING EMAIL ON YOUR SMARTPHONE

If you choose to access a potentially sensitive email account on a mobile device, you should make sure that device encryption is enabled, as discussed in the basic Security for Android guide. (Recent iPhones should have it turned on by default as long as you set a strong passcode.) This will not protect your emails in transit but it will prevent someone who finds or steals your device from reading them. You might also want to read the Tactics Guides on how to keep your online communication private.

The above guide covers GPG email encryption on Windows, Mac and Linux computers. There are ways to send and receive encrypted email on Android devices, as well, but they come with trade-offs. (There are currently no free GPG encryption tools for iOS.)

Most security experts advise against storing your private encryption key anywhere but on your primary computer. (To say nothing of carrying it around in your pocket.) And you will need that private key to read encrypted emails on your mobile device. Android devices are more secure than they used to be, however, and your private key is itself be protected by a strong passphrase. As such, if you must send and receive sensitive email on your Android device — and if switching to a secure mobile messaging app is not an option — you might want to install GPG on it.

To do so, you will need to:

- Install and configure a GPG and key management app like OpenKeychain;
- Copy your encrypted private key to the device; and
- Install and configure an email app, like K-9 Mail, that works with OpenKeychain.

BEYOND CALLS AND MESSAGES

Mobile phones are full featured computing devices, complete with their own operating systems and downloadable applications that provide various services to the user. Much of what you can do on a computer, you can now do on a smartphone. And, of course, there are plenty of things you can do on a smartphone that you cannot do on a computer.

BROWSING THE WEB ON YOUR MOBILE PHONE

While some basic mobile phones still lack Internet connectivity, this is increasingly rare. If you use the Web browser on your Android device to visit potentially sensitive websites, consider installing a virtual private network (VPN) or Orbot, which is the Android version of the Tor Browser.

USING A VPN ON AN ANDROID DEVICE

A VPN provides an encrypted tunnel from your device to a VPN server somewhere on the Internet. VPNs help protect traffic to and from your mobile device, especially when that traffic passes through an insecure local or national network. Because all of your traffic goes through the VPN provider, however, those who operate it can see anything that your local network or Internet service provider would see without it. As a result, it is important to use a VPN service that you trust and to remain vigilant about using only HTTPS services for sensitive information.

VPNs are illegal or restricted in some places, so make sure you are familiar with local policies and practices. Using a VPN does not hide the fact that you are using a VPN.

To use a VPN, you will need to install a "client" application and create an account with a VPN provider. The Riseup Collective offers a FOSS Android VPN client called Bitmask and runs a free VPN service called Riseup Black. (If you already have a Riseup Red account, and are comfortable configuring your VPN manually, you can also use the FOSS OpenVPN for Android app (Play Store, F-Droid) with your Riseup Red username and password.

USING TOR ON AN ANDROID DEVICE

To access online content anonymously, you can use a pair of Android apps called Orbot and Orfox. Orbot channels Internet traffic through Tor's anonymity network and Orfox is a mobile version of Firefox that uses Orbot and provides additional privacy protections. Together, they allow you to circumvent online filtering and browse anonymously, much like Tor Browser on a Windows, Mac or Linux computer.

You can learn more about anonymity and censorship circumvention in the corresponding Tactics Guide.

CAPTURING MEDIA WITH YOUR SMARTPHONE

Taking pictures, recording audio and filming video with your smartphone are all powerful ways to document and share important events. However, it is important to be respectful of the privacy and safety of those who appear in the media you capture. If you document a sensitive event and your phone falls into the wrong hands, for example, it could spell trouble for you and for those who appear in your recordings. To help manage risks like this, you might consider:

Finding a secure way to upload recorded media files, as quickly as possible, and removing them from your device.

Using tools that blur the faces of those who appear in the images and videos you capture or that scramble the voices you record.

Familiarising yourself with tools and device settings that remove metadata from media files. These metadata might include the GPS coordinates at which photos are taken, revealing device identification data or other potentially sensitive data.

The Guardian Project developed and maintains a FOSS app called ObscuraCam that blurs faces and removes metadata from photographs and videos.

If you need to retain the faces, voices and metadata in the media you capture, then it is even more important that you make sure your device is encrypted and that you take care to encrypt the relevant files when storing them elsewhere or sending them to others. With that in mind, the Guardian Project has also developed a tool called Proof Mode that does the opposite of what ObscuraCam does. It collects as much metadata as possible as a way to help prove the validity of an images or videos. These metadata are stored separately from the images and videos they describe, and should only be shared through secure means.

GENERAL PURPOSE BEST PRACTICES FOR MOBILE PHONES

- Only connect your phone to a computer if you are sure it is free of malware. See our Tactics Guide on how to protect your computer from malware and phishing attacks.
- Just as you would when using a computer, be wary when connecting to a WiFi access point that does not ask for a password.
- Disable WiFi, Bluetooth, and Near Field Communication (NFC) when you are not using them. Switch them on only when they are required and use them only on trusted networks and when interacting with trusted devices. Transfer data using a cable connection when possible.
- Observe your phone's behaviour and functioning. Look out for unknown programmes and running processes, strange messages and unstable operation. If you don't know or use some of the features and applications on your phone, disable or uninstall them if you can.

SECURITY-RELATED SETTINGS FOR ANDROID

ACCESS TO YOUR PHONE

Enable Lock SIM card, found under Settings -> Personal -> Security -> Set up SIM card lock. This will mean that you must enter a PIN number in order to unlock your SIM card each time your phone is switched on, with out the PIN no phone calls can be made.

Set up a Screen Lock, found under Settings -> Personal -> Security -> Screen Lock, which will ensure that a code, pattern or password needs to be entered in order to unlock the screen once it has been locked. We recommended using the PIN or Password option, as these are not restricted by length. You can find more information on creating strong passwords in How to create and maintain secure passwords.

Set the security lock timer, which will automatically lock your phone after a specified time. You can specify a value which suits you, depending on how regularly you are willing to have to unlock your phone.

DEVICE ENCRYPTION

If your device uses Android version 4.0 or newer, you should turn on device encryption. This can be done in Settings -> Personal -> Security -> Encryption. Before you can utilise device encryption, however, you will be required to set a screen lock password (described above).

Note: Before starting the encryption process, ensure the phone is fully charged and plugged into a power source.

NETWORK SETTINGS

Turn off Wi-Fi and Bluetooth by default. Ensure that Tethering and Portable Hotspots, under Wireless and Network Settings, are switched off when not in use. Settings -> Wireless & Networks -> More -> Tethering & Mobile hotspot.

If your device supports Near Field Communication (NFC), this will be switched on by default, and so must be switched off manually.

LOCATION SETTINGS

Switch off Wireless and GPS location (under Location Services) and mobile data (this can be found under Settings -> Personal -> Location).

Note: Only turn on location settings as you need them. It is important not have these services running by default in the background as it reduces the risk of location tracking, saves battery power and reduces unwanted data streams initiated by applications running in the background or remotely by your mobile carrier.

CALLER IDENTITY

If you want to hide your caller-ID, go to Phone Dialler -> settings -> Additional Settings -> Caller ID -> hide number.

SOFTWARE UPDATES

To ensure that you phone remains secure it is strongly recommended to keep your software updated. There are two types of updates that need to be checked:

The phone operating system: go to: settings -> About phone -> updates -> check for updates.

Apps you have installed: Open the Play store app, from the side menu select My Apps.

Note: When updating your phones software it is important to do it from a trusted location such as your internet connection at home instead of somewhere like an internet cafe or coffee shop.

APPS FOR ANDROID

RECOMMENDED ANDROID APPS

We have a number of Tools Guides for Android apps that we recommend installing on your device. These guides will walk you through installing, configuring and using the apps on your Android Devices.

APG

License: FOSS (GPL v3) / Requirements: Android 1.5 and up.

Details: lets you encrypt and decrypt single files or emails, for personal use or to share with others, using either public key cryptography or a passphrase.

ChatSecure

License: FOSS (GPLv3) / Requirements: Android 1.6 and up.

Details: Is an Instant Messaging client that lets you organize and manage your different Instant Messaging (IM) accounts using a single interface. It will also attempt to encrypt your conversations using OTR when chatting with contacts who also use IM clients that support OTR.

K-9 Mail and APG

License: FOSS (Apache 2.0) / Requirements: Android 1.5 or up.

Details: K-9 Mail is a mail client that integrates with APG to allow you easily send and receive GnuPG encrypted emails.

KeePassDroid

License: FOSS (GPL v2) / Requirements: Android 1.5 and up.

Details: is a secure and easy-to-use password management tool which will store your passwords in an encrypted database on your phone.

Obscuracam

License: FOSS (GPL v3) / Requirements: Varies by device.

Details: is a free camera application for Android devices that has the ability to recognize and hide faces. It allows you to blur or delete the faces of those you photograph in order to protect their identities.

Orbot

License: FOSS (BSD) / Requirements: Android 2.3 and up.

Details: is an app that is designed to increase the anonymity of your activities on the Internet by sending your connections over the Tor network.

Orweb

License: FOSS (GPL v2) / Requirements: Android 1.6 and up.

Details: is a web browser that is used in conjunction with Orbot, that allows you to send all your web browsing over the Tor network.

Signal

License: FOSS (GPL v3) / Requirements: Android 2.3 and up.

Details: Allows you to exchange encrypted messages and have encrypted voice calls over the internet. A valid phone number is required to register.

ADDITIONAL ANDROID APPS FOR NON-ROOTED DEVICES

Along with the software covered by our Tools Guides for Android, we also suggest the following apps.

Applock

License: Commercial / Requirements: Dependant on device.

Details: Allows you to password protect apps on your phone so that they can not be run with out entering the correct passphrase. For example protect your Mail app with additional passphrase.

Avira

License: Commercial / Requirements: Android 2.2 and up.

Details: Anti-Virus software that will scan your phone for malicious apps and files. It will also allow you to locate your phone if lost.

Cerberus

License: Proprietary / Requirements: Android 4.0.3 and up.

Details: An anti-theft solution that will allow you to locate your phone if lost or stolen. It will also allow you to remotely lock or wipe the contents of your phone.

Firefox

License: FOSS / Requirements: Dependant on device

Details: brings the experience of Firefox Browser for the desktop to your mobile phone.

Notecipher

License: FOSS (Apache v2) / Requirements: Android 3.0 and up.

Details: A note taking application that stores all notes in an encrypted container protected by a passphrase.

OpenVPN for Android

License: FOSS (GPL v2) / Requirements: Android 4.0 and up.

Details: Allows you to tunnel your apps, that connect to the internet, over OpenVPN based VPNs, protecting you from monitoring.

Panic Button

License: FOSS (GPL v3) / Requirements: Android 2.3.3 and up.

Details: Allows you to secretly trigger your phone to send an SMS letting a predefined list of contacts know you may be in danger.

Psiphon3

License: FOSS (GPL v3) / Requirements: Dependant on device.

Details: helps you to try and circumvent censorship and monitoring by tunneling your internet connection over a number of different encrypted tunnel types such as VPNs and Proxies.

Spideroak

License: Proprietary / Requirements: Dependant on device.

Details: is a file synchronisation tool that will allow you to easily share files between your computers and Android devices via an intermediary 3rd party server on the internet. All files are encrypted by the app before being uploaded to the Spideroak servers.

Surespot

License: FOSS (GPL v3+) / Requirements: Android 2.3.3 and up.

Details: an secure messaging app that provides end to end encryption for all messages and files sent. No personal details (phone, email) are required for registration.

ADDITIONAL ANDROID APPS FOR ROOTED DEVICES

The following apps are for advanced users of Android and require your phone to be rooted.

AFwall+

License: FOSS (GPL v3) / Requirements: Android 2.2 and up.

Details: A firewall for your android device that allows you to control what apps can access the internet.

CryptFS

License: FOSS (Apache v2) / Requirements: Android 3.0 and up.

Details: lets you to change your Android disk encryption password meaning you can have a one passphrase to decrypt the phone when you turn it on and a different one to unlock the phone during normal use.

Cryptonite

License: FOSS (GPL v2) / Requirements: Android 2.2 and up.

Details: allows you to create encrypted, passphrase protected, containers on your Android device that you can store sensitive files in.

SnoopSnitch

License: FOSS (GPL v3) / Requirements: Android 4.1 - 4.4 and only specific handsets.

Details: is an Android app that collects and analyses mobile radio data to make you aware of your mobile network security and to warn you about threats like fake base stations (IMSI catchers), user tracking and over-the-air updates.

X-Privacy

License: FOSS (GPL v3) / Requirements: Android 4.0.3 and up.

Details: is an app that will prevent your Android device from leaking sensitive information (such as your phone number, contacts, location, etc) to other installed apps on your phone. While x-privacy is free, there is a Pro version that can be purchased, which allows you to download restriction rules rather than you having to make them your self.

iOS Security

How to Encrypt Your iPhone

If you have an iPhone 3GS or later, an iPod touch 3rd generation or later, or any iPad, you can protect the contents of your device using encryption. That means that if someone gets physical access to your device,

they will also need your passcode to decrypt what's stored on it, including contacts, instant messages or texts, call logs, and email.

In fact, most modern Apple devices encrypt their contents by default, with various levels of protection. But to protect against someone obtaining your data by physically stealing your device, you need to tie that encryption to a passphrase or code that only you know. See below for instructions on how to do this.

On devices running iOS 4–iOS 7:

1. Open the General settings and choose Passcode (or iTouch & Passcode).
2. Follow the prompts to create a passcode.

On device running iOS 8-iOS 11:

1. Open the Settings app
2. Tap Touch ID & Passcode
3. Follow the prompts to create a passcode.

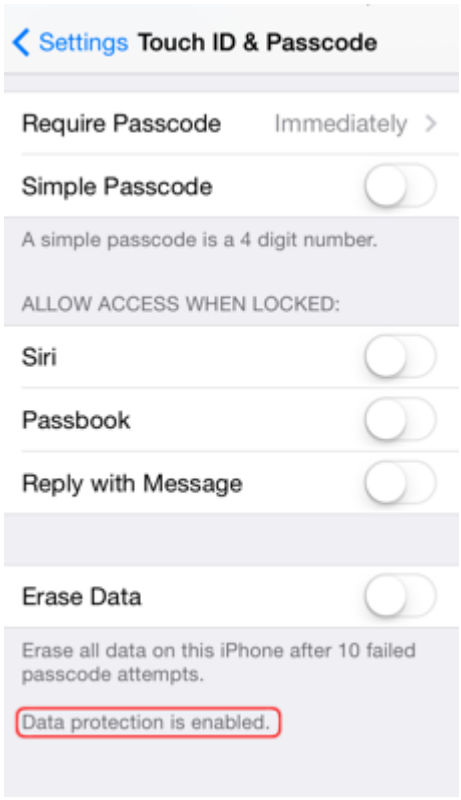
If your device is running iOS 8, disable Simple Passcode to create a code that is longer than 4 digits. With the release of iOS 9, Apple defaulted to a 6-digit passcode.

If you choose a passcode that's all-numeric, you will get a numeric keypad when you need to unlock your phone, which may be easier than typing a set of letters and symbols on a tiny virtual keyboard. However, we suggest choosing a passcode that's alphanumeric, and longer than 6 characters because it's simply harder to crack, even if Apple's hardware is designed to slow down password-cracking tools.

To customize your passcode, select "Passcode Options" and "Custom Alphanumeric Code." If you want to customize an existing passcode, select “Change Passcode” and then “Passcode Options.” You should also set the “Require passcode” option to “Immediately,” so that your device isn't unlocked when you are not using it.

Once you've set a passcode, scroll down to the bottom of the Passcode settings page. You should see a message that says “Data protection is enabled.” This means that the device's encryption is now tied to your passcode, and that most data on your phone will need that code to unlock it.

How to Encrypt Your iPhone 1



Here are some other iOS features you should think about using if you're dealing with private data:

- iTunes has an option to backup your device onto your computer. iTunes doesn't encrypt your backups by default. If you choose the “Encrypt backup” option on the Summary tab of your device in iTunes, iTunes will backup more confidential information (such as Wi-Fi passwords and email passwords), but will encrypt it all before saving it onto your computer. Be sure to keep the password you use here safe: restoring from backups is a rare event, but extra painful if you cannot remember the password to unlock the backup in an emergency.
- If you back up to Apple's iCloud, you should use a long passphrase to protect the data, and keep that passphrase safe. While Apple encrypts most data in its backups, it may be possible for the company to obtain access for law enforcement purposes since Apple also controls the keys used for iCloud encryption.
- If you turn on data protection as described above, you will also be able to delete your data on your device securely and quickly. In the Touch ID & Passcode settings, you can set your device to erase all its data after 10 failed passcode attempts. If you do this be sure your phone is backed up in case someone purposefully enters your passcode incorrectly.
- According to Apple’s old Law Enforcement Guide, “Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple’s native apps and for which the data is not encrypted using the passcode (“user generated active files”), can be extracted and provided to law enforcement on external media. Apple can perform this data extraction process on iOS devices running iOS 4 or more recent versions of iOS. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant

to a valid search warrant, are: SMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party App data."

The above information applies only to iOS devices running versions of iOS prior to 8.0.

- Now, Apple states that "For all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key."

REMEMBER: While Apple will be unable to extract data directly off a phone, if the device is set to sync with iCloud, or backup to a computer, much of the same data will indeed be accessible to law enforcement. Under most circumstances, iOS encryption is only effective when a device has been fully powered down (or freshly-rebooted, without being unlocked). Some attackers might be able to take valuable data from your device's memory when it's turned on. (They might even be able to take the data when it has just been turned off). Keep this in mind and, if possible, try to make sure your device is powered off (or rebooted and not unlocked) if you believe it's likely to be seized or stolen. At the time this guide was published, a few companies claimed they were able to break the passcodes of iPhones for law enforcement, but details surrounding these claims are unclear.

- If you are concerned about your device getting lost or stolen, you can also set up your Apple device so that it can be erased remotely, using the "Find My iPhone" feature. Note that this will allow Apple to remotely request the location of your device at any time. You should balance the benefit of deleting data if you lose control of your device, with the risk of revealing your own position. (Mobile phones transmit this information to telephone companies as a matter of course; Wi-Fi devices like iPads and the iPod Touch do not.)

Password policy

GENERATING SECURE PASSWORD

Guideline for setting secure Password

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

Basics

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult to remember.
- Use a random mixture of characters, upper and lower case, numbers, punctuation, spaces and symbols.
- Don't use a word found in a dictionary, English or foreign.

- Never use the same password twice.

Things to avoid

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

Tips

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

Bad Passwords

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

Choosing a password

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

Changing your password

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

Protecting your password

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

Remembering your password

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

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

Bad Examples

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

Good Examples

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

- "mItWdOtW4Me" - 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 should 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.

Two step authentication process

How to Set up 2 Step Verification in Gmail

Two-Step Verification is an additional layer of security that you can add onto your Gmail account. When enabled, you will have to enter your password, and enter a special code that is sent to your device, or verify the sign in attempt on your phone. This dramatically increases the security of your account and makes sure that hackers can't get into your account even if the guess or steal your password. This wikiHow teaches you how to enable two-step verification on Gmail.

Method 1 Text Message or Voice Call

1 Decide if you want to use the text message or voice call option. With this enabled, a code will be sent to your phone via text, or Google will call your phone and tell you the code. You then enter this code into the sign in prompt in order to sign in.

USING PASSWORD MANAGER

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. 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.

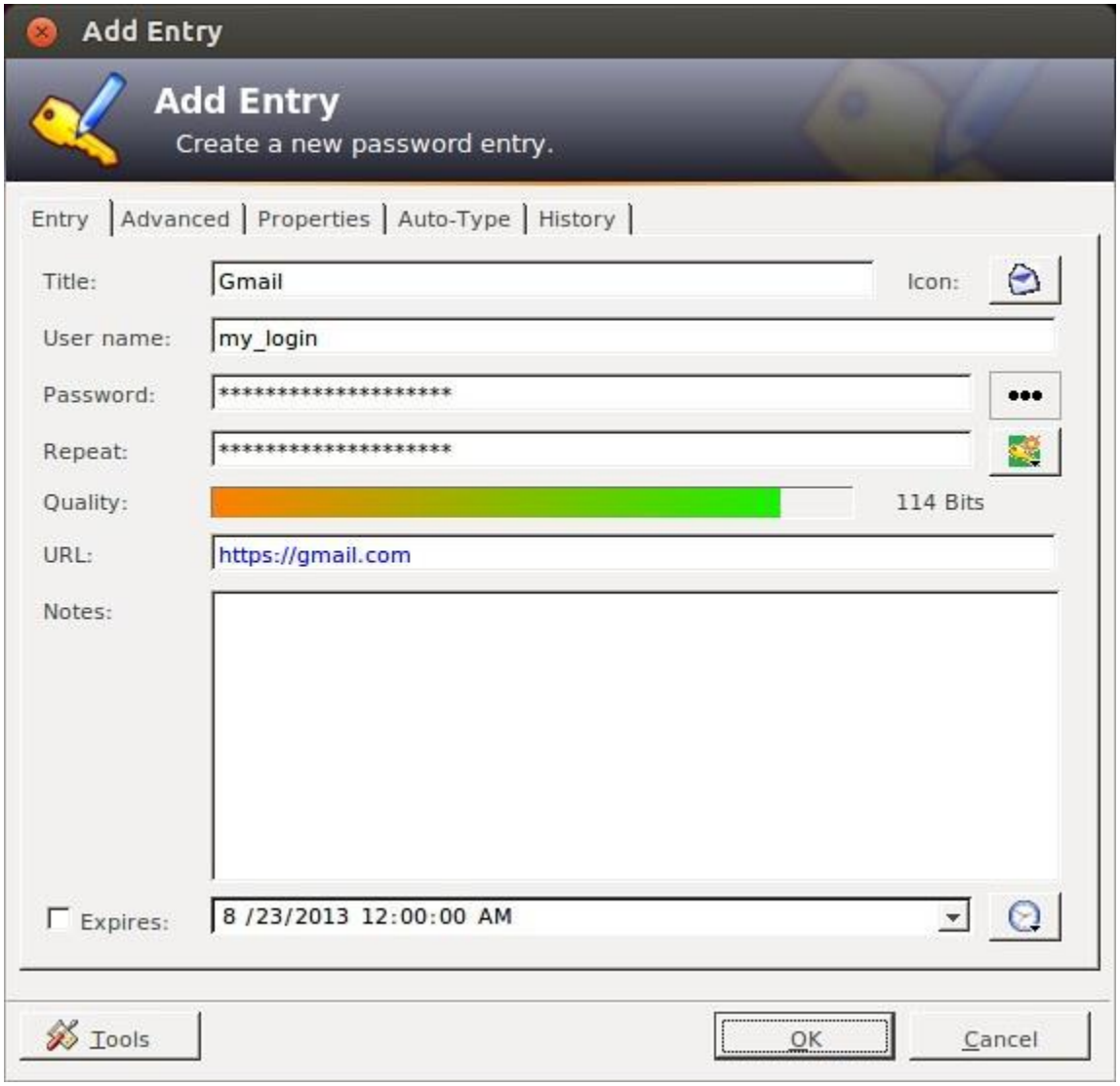
Online password managers use browser extensions that keep data in a local profile, syncing with a cloud server. Some other password managers use removable media to save the password so that you can carry it with you and don't have to worry about online issues. Both these options can also be combined and used as two-factor authentication so that data is even more secure.

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.



KeePassX [Image Courtesy: https://www.flickr.com/photos/xmodulo/9580944074]

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.

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.

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.

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.

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

How the attack occurs in Wifi Environment ?

- At the physical layer of TCP/IP Model, denial of service attack can be implemented by introducing a device which will generate noise in the same frequency band in which wireless accesspoint is operating. This makes the users who are trying to connect to the accesspoint may not be able to connect to it.
- Also the other possibility of Denial of service Attack is spoofing the accesspoint. Normally wireless clients connect to the wired network with the help of an accespoint.
  For associating with the accesspoint they require SSID of it. When an unauthorised user places an accesspoint with the same SSID, then there is a chance of authorised user getting associated with the attackers accesspoint. If that happens, the attacker will try to collect sufficient number of packets from the wireless client and cracks the WEP key used by the legitimate accesspoint. Then the attacker gets associated with the legitimate accesspoint and generates large ping requests in the network or generate some abnormal traffic, which may finally result in Denial of Service Attack.

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.

_____

Adopted from: https://infosecawareness.in/infosec-concept/wi-fi-security

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 malware detection, malware quarantine & removal, etc. It can be downloaded from http://www.threatfire.com/download/

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.