**EFF Glossary**

[**Adversary**](https://ssd.eff.org/en/glossary/adversary)

Your [adversary[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/adversary)](https://ssd.eff.org/en/glossary/adversary) is the person or organization attempting to undermine your security goals. Adversaries can be different, depending on the situation. For instance, you may worry about criminals spying on the network at a cafe, or your classmates at a school. Often the adversary is hypothetical.

[**Air gap**](https://ssd.eff.org/en/glossary/air-gap)

A computer or network that is physically isolated from all other networks, including the Internet, is said to be air-gapped.

[**Anti-virus**](https://ssd.eff.org/en/glossary/anti-virus)

Software that attempts to protect a device from being taken over by [malicious software[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/malware)](https://ssd.eff.org/en/glossary/malware) (or “[malware[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/malware)](https://ssd.eff.org/en/glossary/malware)"). "Viruses' were some of the first and most prevalent forms of malware; they were named viruses to reflect the way they would spread from device to device. These days most antivirus software concentrate on warning you if you look to be downloading a suspicious fiile from an external source, and examining files on your computer to see if they match the software's idea of what malware looks like.

[Anti-virus[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/anti-virus)](https://ssd.eff.org/en/glossary/anti-virus) software can only recognise malware if it is substantially similar to samples that the anti-virus developer has already analysed. This makes it far less effective at combating targeted malware designed to infiltrate a particular community or person, rather than more widespread strains of malware. Some advanced malware can also actively [attack[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/attack)](https://ssd.eff.org/en/glossary/attack) or conceal itself from antivirus software.

[**Asset**](https://ssd.eff.org/en/glossary/asset)

In [threat modeling[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/threat-model)](https://ssd.eff.org/en/glossary/threat-model), any piece of data or a device that needs to be protected.

[**Attack**](https://ssd.eff.org/en/glossary/attack)

In computer security, an [attack[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/attack)](https://ssd.eff.org/en/glossary/attack) is a method that can be used to compromise security, or its actual use. An attacker is the person or organization using an attack. An attack method is sometimes called an "exploit."

[**Burner phone**](https://ssd.eff.org/en/glossary/burner-phone)

A phone that is not connected to your identity, is only used for a small set of calls or activities, and can be discarded if and when it is suspected of being tracked or compromised. Burner phones are often pre-paid mobile phones bought with cash.

[**Command line tool**](https://ssd.eff.org/en/glossary/command-line-tool)

The "command line" is an ancient way of giving a computer a series of small, self-contained orders (think of those science fiction movies where teenage geniuses type long strings of green text onto black screens). To use a[command line tool[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/command-line-tool)](https://ssd.eff.org/en/glossary/command-line-tool), the user types a command into a window called a[terminal[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/terminal)](https://ssd.eff.org/en/glossary/terminal) emulator, hits the return or enter [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key), and then receives a textual response in the same window. Windows, Linux and Apple desktop computers still let you run software using this interface, and even some mobile phones can do the same with the right app. The command line can be used to run software pre-packaged with your [operating system[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/operating-system)](https://ssd.eff.org/en/glossary/operating-system). Some downloadable programs, especially technical utilities, use the command line instead of a more familiar "icons and buttons" user interface. The command line needn't be scary, but it does require you to type in exactly the right set of letters and numbers to get the correct result, and it's often unclear what to do if the responses don't match your expectations.

[**Commercial VPN**](https://ssd.eff.org/en/glossary/commercial-vpn)

A commercial [Virtual Private Network[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/virtual-private-network)](https://ssd.eff.org/en/glossary/virtual-private-network) is a private service that offers to securely relay your Internet communications via their own network. The advantage of this is that all of the data you send and receive is hidden from local networks, so it is safer from nearby criminals, or untrusted local ISPs or cybercafes. A [VPN[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/virtual-private-network)](https://ssd.eff.org/en/glossary/virtual-private-network) may be hosted in a foreign country, which is useful both for protecting communications from a local government, and bypassing national censorship. The down side is that most of the traffic is decrypted at the [commercial VPN[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/commercial-vpn)](https://ssd.eff.org/en/glossary/commercial-vpn)'s end. That means you need to trust the commercial VPN (and the country where it is located) not to snoop on your traffic.

[**Cookies**](https://ssd.eff.org/en/glossary/cookies)

[Cookies[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/cookies)](https://ssd.eff.org/en/glossary/cookies) are a web technology that let websites recognize your browser. Cookies were originally designed to allow sites to offer online shopping carts, save preferences or keep you logged on to a site. They also enable tracking and profiling so sites can recognize you and learn more about where you go, which devices you use, and what you are interested in – even if you don't have an account with that site, or aren't logged in.

[**Corporate Intranet**](https://ssd.eff.org/en/glossary/corporate-intranet)

Companies and other large institutions will usually have some services (email, web, and access to files and printers for instance) that are accessible from within their own local network, but not from outside on the wider Internet. Most companies take this as being sufficient security to protect their internal documents, but this means that any [attack[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/attack)](https://ssd.eff.org/en/glossary/attack) that can connect to the intranet can access or interfere with all the information being kept locally. An example of such an attack is tricking an employee to install [malware[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/malware)](https://ssd.eff.org/en/glossary/malware) on their laptop.

To allow employees to access the intranet via the wider Internet, companies will often provide their own [Virtual Private Network[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/virtual-private-network)](https://ssd.eff.org/en/glossary/virtual-private-network) ([VPN[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/virtual-private-network)](https://ssd.eff.org/en/glossary/virtual-private-network)) which creates a secure connection to the inside of the intranet from anywhere in the world.

[**Cryptography**](https://ssd.eff.org/en/glossary/cryptography)

The art of designing secret codes or ciphers that let you send and receive messages to a recipient without others being able to understand the message.

[**Decrypt**](https://ssd.eff.org/en/glossary/decrypt)

Make a secret message or data intelligible. The idea behind [encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/encryption)](https://ssd.eff.org/en/glossary/encryption) is to make messages that can only be decrypted by the person or people who are meant to receive them.

[**Distributed Denial of Service attack**](https://ssd.eff.org/en/glossary/distributed-denial-service-attack)

A method for taking a website or other Internet service offline, by co-ordinating many different computers to request or send data to it simultaneously. Usually the computers used to conduct such an [attack[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/attack)](https://ssd.eff.org/en/glossary/attack) are remotely controlled by criminals, who have taken over the machines by breaking into them, or infecting them with [malware[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/malware)](https://ssd.eff.org/en/glossary/malware).

[**Domain name**](https://ssd.eff.org/en/glossary/domain-name)

The address, in words, of a website or Internet service; for example: ssd.eff.org

[**Encryption**](https://ssd.eff.org/en/glossary/encryption)

A process that takes a message and makes it unreadable except to a person who knows how to "[decrypt[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/decrypt)](https://ssd.eff.org/en/glossary/decrypt)" it back into a readable form.

[**Encryption key**](https://ssd.eff.org/en/glossary/encryption-key)

An [encryption key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/encryption-key)](https://ssd.eff.org/en/glossary/encryption-key) is a piece of information that is used to convert a message into an unreadable form. In some cases, you need the same encryption key to decode the message. In others, the encryption key and decryption [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key) are different.

[**End-to-end encryption**](https://ssd.eff.org/en/glossary/end-end-encryption)

[End-to-end encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/end-end-encryption)](https://ssd.eff.org/en/glossary/end-end-encryption) ensures that a message is turned into a secret message by its original sender, and decoded only by its final recipient. Other forms of [encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/encryption)](https://ssd.eff.org/en/glossary/encryption) may depend on encryption performed by third-parties. That means that those parties have to be trusted with the original text. End-to-end encryption is generally regarded as safer, because it reduces the number of parties who might be able to interfere or break the encryption.

[**File system**](https://ssd.eff.org/en/glossary/file-system)

Where data is stored, usually locally, on your computer or other device. File systems are usually where personal documents and notes are stored for easy access.

[**File Transfer Protocol (FTP server)**](https://ssd.eff.org/en/glossary/file-transfer-protocol-ftp-server)

An old method for copying files from a local computer to a remote one, or vice versa. The job of FTP programs (and the FTP servers that stored the files) have mostly been replaced by web browsers and web servers, or file synchronising programs like Dropbox.

[**Firewall**](https://ssd.eff.org/en/glossary/firewall)

A tool that protects a computer from unwanted connections to or from local networks and the Internet. A [firewall[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/firewall)](https://ssd.eff.org/en/glossary/firewall) might have rules that forbid outgoing email, or connections to certain websites. Firewalls can be used as a first line of defense to protect a device from unexpected interference. Or they can be used to prevent users from using the Internet in certain ways.

[**Forward secrecy**](https://ssd.eff.org/en/glossary/forward-secrecy)

A property of a secure messaging system which ensures that your past  
communications can remain secure even if one of the private keys is stolen  
later.

For [HTTPS[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/https)](https://ssd.eff.org/en/glossary/https) websites, [forward secrecy[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/forward-secrecy)](https://ssd.eff.org/en/glossary/forward-secrecy) is an important protection against  
adversaries like intelligence agencies which may record large amounts of  
traffic and use a stolen [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key) to [decrypt[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/decrypt)](https://ssd.eff.org/en/glossary/decrypt) it. For instant messaging and  
chat systems, forward secrecy is necessary to ensure that deleted  
messages are really deleted, but you will also need to either  
[disabled logging] or [securely delete past messages].

[**Free, libre and open source software**](https://ssd.eff.org/en/glossary/free-libre-and-open-source-software)

Open source software, or free software, is software that can be distributed freely in a form that lets others modify it and rebuild it from scratch. While it is known as “free software”, it's not necessarily free as in zero-cost: [FLOSS[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/free-libre-and-open-source-software)](https://ssd.eff.org/en/glossary/free-libre-and-open-source-software)programmers can ask for donations, or charge for support or for copies. Linux is an example of a free, open source program, as are Firefox and Tor.

[**Full disk encryption**](https://ssd.eff.org/en/glossary/full-disk-encryption)

If you're planning on securing data on your local device, you could choose to just encrypt a few [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key) files, or you could encrypt everything on the computer. “[Full disk encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/full-disk-encryption)](https://ssd.eff.org/en/glossary/full-disk-encryption)” is the term for encrypting everything. It's usually safer (and often easier) to use full disk encryption than to manage just a few individually encrypted files. If you try to encrypt just individual files, your computer might make temporary unencrypted copies of those files without you noticing. And some software might keep some unencrypted records about your use of your computer. Apple's OS X, Linux and high-end versions of Windows all have built-in full disk encryption, but it is usually not turned on by default.

[**HTTPS**](https://ssd.eff.org/en/glossary/https)

If you've ever seen a web address spelled out as “<http://www.example.com/>”, you'll recognize the “http” bit of this term. HTTP (hypertext transfer [protocol[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/protocol)](https://ssd.eff.org/en/glossary/protocol)) is the way a [web browser[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/web-browser)](https://ssd.eff.org/en/glossary/web-browser) on your machine talks to a remote web server. Unfortunately, standard http sends text insecurely across the Internet. [HTTPS[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/https)](https://ssd.eff.org/en/glossary/https)(the S stands for “secure”) uses [encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/encryption)](https://ssd.eff.org/en/glossary/encryption) to better protect the data you send to websites, and the information they return to you, from prying eyes.

[**IMAP settings**](https://ssd.eff.org/en/glossary/imap-settings)

IMAP is the way that many email programs communicate with services that send, receive and store your email. By changing the [IMAP settings[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/imap-settings)](https://ssd.eff.org/en/glossary/imap-settings) on your email program, you can choose to load email from different servers or set the level of security and [encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/encryption)](https://ssd.eff.org/en/glossary/encryption) used to transfer the mail across the Internet to you.

[**Indicators of compromise**](https://ssd.eff.org/en/glossary/indicators-compromise)

Clues that show that your device may have been broken into or tampered with.

[**Internet filtering**](https://ssd.eff.org/en/glossary/internet-filtering)

Filtering is the politer term for [blocking[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/internet-filtering)](https://ssd.eff.org/en/glossary/internet-filtering) or censoring Internet traffic.

[**IP address**](https://ssd.eff.org/en/glossary/ip-address)

A device on the Internet needs its own address to receive data, just like a home or business needs a street address to receive physical mail. This address is its IP (Internet [Protocol[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/protocol)](https://ssd.eff.org/en/glossary/protocol)) address. When you connect to a web site or other server online, you usually reveal your own [IP address[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/ip-address)](https://ssd.eff.org/en/glossary/ip-address). This doesn't necessarily reveal either your identity (it's hard to map an IP address to a real address or a particular computer). An IP address can give away some information about you, however, such as your rough location or the name of your Internet Service Provider. Services like Tor let you hide your IP address, which helps give you anonymity online.

[**Key**](https://ssd.eff.org/en/glossary/key)

In [cryptography[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/cryptography)](https://ssd.eff.org/en/glossary/cryptography), a piece of data which gives you the capability to encrypt or[decrypt[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/decrypt)](https://ssd.eff.org/en/glossary/decrypt) a message.

[**Key pair**](https://ssd.eff.org/en/glossary/key-pair)

To receive encrypted messages using [public key cryptography[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key-verification)](https://ssd.eff.org/en/glossary/key-verification) (and to reliably inform others that a message genuinely came from you), you need to create two keys. One, the private [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key), you keep secret. The other, the public key, you can let anyone see. The two keys are connected mathematically, and are often collectively known as a "keypair".

[**Key verification**](https://ssd.eff.org/en/glossary/key-verification)

In [public key cryptography[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key-verification)](https://ssd.eff.org/en/glossary/key-verification), each person has a set of keys. To send a message securely to a particular person, you encrypt your message using their public[key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key). An attacker may be able to trick you into using their key, which means that they will be able to read your message, instead of the intended recipient. That means that you have to verify that a key is being used by a particular person. [Key verification[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key-verification)](https://ssd.eff.org/en/glossary/key-verification) is any way that lets you match a key to a person.

[**Key-signing party**](https://ssd.eff.org/en/glossary/key-signing-party)

When you're using [public key encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/public-key-encryption)](https://ssd.eff.org/en/glossary/public-key-encryption), it's important to be sure that the[key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key) you use to encrypt a message really belongs to the recipient (see [key verification[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key-verification)](https://ssd.eff.org/en/glossary/key-verification)). [PGP[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp) makes this a little easier by having a way to tell others "I believe this key belongs to this person -- and if you trust me, you should believe that too." Telling the world that you trust someone's key is called "signing their key": it means anyone who uses that key can see you vouched for it. To encourage everyone to check and sign each others keys, PGP users organize [key-signing parties[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key-signing-party)](https://ssd.eff.org/en/glossary/key-signing-party). They're almost, but not quite, as exciting as they sound.

[**Keylogger**](https://ssd.eff.org/en/glossary/keylogger)

A malicious program or device that records everything you type into a device, including passwords and other personal details, allowing others to secretly collect that information. (The "[key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key)" in [keylogger[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/keylogger)](https://ssd.eff.org/en/glossary/keylogger) refers to the keys you have on your keyboard.) Keyloggers are often [malware[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/malware)](https://ssd.eff.org/en/glossary/malware) that users have been tricked into downloading and running, or occasionally physical hardware secretly plugged into a keyboard or device.

[**Keyring**](https://ssd.eff.org/en/glossary/keyring)

If you use [public key cryptography[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key-verification)](https://ssd.eff.org/en/glossary/key-verification), you'll need to keep track of many keys: your secret, private [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key), your public key, and the public keys of everyone you communicate with. The collection of these keys is often referred to as your[keyring[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/keyring)](https://ssd.eff.org/en/glossary/keyring).

[**Malware**](https://ssd.eff.org/en/glossary/malware)

[Malware[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/malware)](https://ssd.eff.org/en/glossary/malware) is short for [malicious software[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/malware)](https://ssd.eff.org/en/glossary/malware): programs that are designed to conduct unwanted actions on your device. Computer viruses are malware. So are programs that steal passwords, secretly record you, or delete your data.

[**Man-in-the-middle attack (MITM)**](https://ssd.eff.org/en/glossary/man-middle-attack-mitm)

Suppose you believe you were speaking to your friend, Bahram, via encrypted instant messager. To check it's really him, you ask him to tell you the city where you first met. "Istanbul" comes the reply. That's correct! Unfortunately, without you or Bahram knowing, someone else online has been intercepting all your communications. When you first connected to Bahram, you actually connected to this person, and she, in turn, connected to Bahram. When you think you are asking Bahram a question, she receives your message, relays the question to Bahram, receives his answer back , and then sends it to you. Even though you think you are communicating securely with Bahram, you are, in fact, only communicating securely with the spy, who is also communicating securely to Bahram! This is the man-in-the-middle [attack[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/attack)](https://ssd.eff.org/en/glossary/attack). Men-in-the-middle can spy on communications or even insert false or misleading messages into your communications. Security-focused internet communications software needs to defend against the man-in-the-middle attack to be safe against attackers who have control of any part of the Internet between two communicators.

[**Master password**](https://ssd.eff.org/en/glossary/master-password)

A password used to unlock a store of other passwords or other ways to unlock programs or messages. You should make a [master password[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/master-password)](https://ssd.eff.org/en/glossary/master-password) as strong as you can.

[**Metadata**](https://ssd.eff.org/en/glossary/metadata)

[Metadata[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/metadata)](https://ssd.eff.org/en/glossary/metadata) (or "data about data") is everything about a piece of information, apart from the information itself. So the content of a message is not metadata, but who sent it, when, where from, and to whom, are all examples of metadata. Legal systems often protect content more than metadata: for instance, in the United States, law enforcement needs a warrant to listen to a person's telephone calls, but claims the right to obtain the list of who you have called far more easily. However, metadata can often reveal a great deal, and will often need to be protected as carefully as the data it describes.

[**Off-the-Record (OTR)**](https://ssd.eff.org/en/glossary/record-otr)

Instant messaging systems are often unencrypted. [OTR[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/record-otr)](https://ssd.eff.org/en/glossary/record-otr) is a way of adding[encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/encryption)](https://ssd.eff.org/en/glossary/encryption) to them, so that you can keep using familiar networks like Facebook chat, Google Chat or Hangouts, or Microsoft Messenger, but with your messages more resistant to surveillance.

[**One-time password**](https://ssd.eff.org/en/glossary/one-time-password)

Passwords are usually semi-permanent: once you set them up, you can keep using them until you manually change or reset them. One-time passwords only work once. Some [one-time password[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/one-time-password)](https://ssd.eff.org/en/glossary/one-time-password) systems work by having a tool or program that can create many different one-time passwords, that you use in turn. This is useful if you're afraid that there may be a [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key)-logger on a system where you have to type in a password.

[**Operating system**](https://ssd.eff.org/en/glossary/operating-system)

A program that runs all the other programs on a computer. Windows, Android and Apple's OS X and iOS are all examples of operating systems.

[**Out-of-band verification**](https://ssd.eff.org/en/glossary/out-band-verification)

"Out-of-band" means any way of communicating outside of the current method. Verifying the identity of the person you're talking to over an insecure communication system often requires communicating out-of-band via another method that is less vulnerable to the same kind of [attack[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/attack)](https://ssd.eff.org/en/glossary/attack). So, for instance, you might check that you are using someone's correct public [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key)by talking to them in person, before using it to encrypt your email.

[**Passive adversary**](https://ssd.eff.org/en/glossary/passive-adversary)

A [passive adversary[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/passive-adversary)](https://ssd.eff.org/en/glossary/passive-adversary) is one that can listen to your communications, but cannot directly tamper with them.

[**Passphrase**](https://ssd.eff.org/en/glossary/passphrase)

A [passphrase[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/passphrase)](https://ssd.eff.org/en/glossary/passphrase) is a kind of password. We use "passphrase" to convey the idea that a password which is a single word is far too short to protect you and a longer phrase is much better. The webcomic XKCD has a good explaination.<http://xkcd.com/936/>

[**Password manager**](https://ssd.eff.org/en/glossary/password-manager)

A tool that can encrypt and store your passwords using a single [master password[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/master-password)](https://ssd.eff.org/en/glossary/master-password) making it practical to use many different passwords on different sites and services without having to memorize them.

[**PGP**](https://ssd.eff.org/en/glossary/pgp)

[PGP[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp) or [Pretty Good Privacy[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp) was one of the first popular implementations of[public key cryptography[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key-verification)](https://ssd.eff.org/en/glossary/key-verification). Phil Zimmermann, its creator, wrote the program in 1991 to help activists and others protect their communications. He was formally investigated by the US government when the program spread outside the United States. At the time, exporting tools that included strong [public key encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/public-key-encryption)](https://ssd.eff.org/en/glossary/public-key-encryption) was a violation of US law.

PGP continues to exist as a commercial software product. A free implementation of the same underlying standard that PGP uses called GnuPG (or GPG) is also available. Because both use the same interchangeable approach, people will refer to using a “PGP [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key)” or sending a “PGP message”, even if they are using GnuPG.

[**Protocol**](https://ssd.eff.org/en/glossary/protocol)

A communications [protocol[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/protocol)](https://ssd.eff.org/en/glossary/protocol) is a way of sending data between programs or computers. Software programs that use the same protocol can talk to each other: so web browsers and web servers speak the same protocol, called "http". Some protocols use [encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/encryption)](https://ssd.eff.org/en/glossary/encryption) to protect their contents. The secure version of the http protocol is called "[https[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/https)](https://ssd.eff.org/en/glossary/https)". Another example of an encrypted protocol used by many different programs is [OTR[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/record-otr)](https://ssd.eff.org/en/glossary/record-otr) (Off-the-Record), a protocol for secure instant messaging.

[**Public key encryption**](https://ssd.eff.org/en/glossary/public-key-encryption)

Traditional [encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/encryption)](https://ssd.eff.org/en/glossary/encryption) systems use the same secret, or [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key), to encrypt and[decrypt[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/decrypt)](https://ssd.eff.org/en/glossary/decrypt) a message. So if I encrypted a file with the password "bluetonicmonster", you would need both the file and the secret "bluetonicmonster" to decode it. [Public key encryption[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/public-key-encryption)](https://ssd.eff.org/en/glossary/public-key-encryption) uses two keys: one to encrypt, and other to decrypt. This has all kinds of useful consequences. For one, it means that you can hand out the key to encrypt messages to you, and as long as you keep the other key secret, anyone with that key can talk to you securely. The key you hand out widely is known as the "public key": hence the name of the technique. Public key encryption is used to encrypt email and files by [Pretty Good Privacy[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp) ([PGP[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/pgp)](https://ssd.eff.org/en/glossary/pgp)), [OTR[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/record-otr)](https://ssd.eff.org/en/glossary/record-otr) for instant messaging, and [SSL/TLS[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/secure-sockets-layer-ssl)](https://ssd.eff.org/en/glossary/secure-sockets-layer-ssl)for web browsing.

[**Revocation certificate**](https://ssd.eff.org/en/glossary/revocation-certificate)

What happens if you lose access to a secret [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key), or it stops being secret? A[revocation certificate[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/revocation-certificate)](https://ssd.eff.org/en/glossary/revocation-certificate) is a file that you can generate that announces that you no longer trust that key. You generate it when you still have the secret key, and keep it for any future disaster.

[**Risk analysis**](https://ssd.eff.org/en/glossary/risk-analysis)

In computer security, [risk analysis[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/risk-analysis)](https://ssd.eff.org/en/glossary/risk-analysis) is calculating the chance that threats might succeed, so you know how much effort to spend defending against them. There may be many different ways that you might lose control or access to your data, but some of them are less likely than others. Assessing [risk[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/risk-analysis)](https://ssd.eff.org/en/glossary/risk-analysis)means deciding which threats you are going to take seriously, and which may be too rare or too harmless (or too difficult to combat) to worry about. See[threat modeling[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/threat-model)](https://ssd.eff.org/en/glossary/threat-model).

[**Secure Sockets Layer (SSL)**](https://ssd.eff.org/en/glossary/secure-sockets-layer-ssl)

The technology that permits you to maintain a secure, encrypted connection between your computer and some of the websites and Internet services that you visit. When you are connected to a website through SSL, the address of the website will begin with [HTTPS[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/https)](https://ssd.eff.org/en/glossary/https) rather than HTTP.

[**Security certificate**](https://ssd.eff.org/en/glossary/security-certificate)

A [security certificate[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/security-certificate)](https://ssd.eff.org/en/glossary/security-certificate) is a kind of private [key[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/key)](https://ssd.eff.org/en/glossary/key) used to prevent man-in-the-middle attacks. A site that has access to the certificate can prove to remote systems that it has the certificate, and at the same time demonstrate that no other system without that certificate is tampering with the communication.

[**Security question**](https://ssd.eff.org/en/glossary/security-question)

To supplement passwords, some systems use "security questions". These are queries to which only you are supposed to know the answer. The problem with security questions is that they are really just extra passwords that have potentially guessable answers. We recommend you treat them as any other password: create a long, novel, random, phrase to answer them, and record that somewhere safe. So the next time your bank asks you your mother's maiden name, you should be ready to answer "Correct Battery Horse Staple" or similar.

[**SIM card**](https://ssd.eff.org/en/glossary/sim-card)

A small, removable card that can be inserted into a mobile phone in order to provide service with a particular mobile phone company. SIM (subscriber identity module) cards can also store phone numbers and text messages.

[**SMTP settings**](https://ssd.eff.org/en/glossary/smtp-settings)

SMTP is one method for sending mail between computers. You can configure most email programs to encrypt messages between your e-mail software and the email server by changing your programs' [SMTP settings[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/smtp-settings)](https://ssd.eff.org/en/glossary/smtp-settings) (as long as your email service supports it)

[**Solid State Drive (SSD)**](https://ssd.eff.org/en/glossary/solid-state-drive-ssd)

Historically, computers stored data on rotating magnetic discs. Mobile devices and increasing numbers of personal computers now store permanent data on non-moving drives. These SSD drives are currently more expensive, but much faster than magnetic storage. Unfortunately, it can be more difficult to reliably and permanently remove data from SSD drives.

[**SSH**](https://ssd.eff.org/en/glossary/ssh)

[SSH[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/ssh)](https://ssd.eff.org/en/glossary/ssh) (or Secure SHell) is a method for letting you securely control a remote computer via a command line interface. One of the features of the SSH[protocol[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/protocol)](https://ssd.eff.org/en/glossary/protocol) is that as well as sending commands, you can also use it to securely relay Internet traffic between two computers. To set up an ssh link, the remote system needs to operate as a ssh server, and your local machine need an ssh client program.

[**Terminal**](https://ssd.eff.org/en/glossary/terminal)

In ancient computer history, a [terminal[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/terminal)](https://ssd.eff.org/en/glossary/terminal) was a dedicated system of keyboard and screen that connected a user to a server. These days, it's more likely to be a program that allows you to talk to computers (either local or remote) over the command line.

[**Threat**](https://ssd.eff.org/en/glossary/threat)

In computer security, a [threat[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/threat)](https://ssd.eff.org/en/glossary/threat) is a potential event that could undermine your efforts to defend your data. Threats can be intentional (conceived by attackers), or they could be accidental (you might leave your computer turned on and unguarded).

[**Threat model**](https://ssd.eff.org/en/glossary/threat-model)

A way of narrowly thinking about the sorts of protection you want for your data. It's impossible to protect against every kind of trick or attacker, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. Coming up with a set of possible attacks you plan to protect against is called [threat modeling[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/threat-model)](https://ssd.eff.org/en/glossary/threat-model). Once you have a [threat model[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/threat-model)](https://ssd.eff.org/en/glossary/threat-model), you can conduct a [risk analysis[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/risk-analysis)](https://ssd.eff.org/en/glossary/risk-analysis).

[**Throwaway address**](https://ssd.eff.org/en/glossary/throwaway-address)

An email address you use once, and never again. Used to sign up to Internet services without revealing an email address connected to your identity.

[**Traffic-blocking browser extension**](https://ssd.eff.org/en/glossary/traffic-blocking-browser-extension)

When you visit a website, your browser sends some information to that site's operators -- your [IP address[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/ip-address)](https://ssd.eff.org/en/glossary/ip-address), other information about your computer, and[cookies[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/cookies)](https://ssd.eff.org/en/glossary/cookies) that link you to previous visits using that browser, for instance. If the website includes images and content taken from other web servers, that same information is sent to other websites as part of downloading or viewing the page. Advertising networks, analytics providers, and other data collectors may gather information from you in this way.

You can install additional software that tuns alongside your browser and will limit how much information is leaked to third-parties in this way. The most well-known examples are programs that block advertisements. EFF offers a tool called [Privacy Badger](https://www.eff.org/privacybadger) which is another traffic-[blocking[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/internet-filtering)](https://ssd.eff.org/en/glossary/internet-filtering) extension.

[**Transport encryption**](https://ssd.eff.org/en/glossary/transport-encryption)

Encrypting data as it travels across the network, so that others spying on the network cannot read it.

[**Two-factor authentication**](https://ssd.eff.org/en/glossary/two-factor-authentication)

"Something you know, and something you have." Login systems that require only a username and password [risk[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/risk-analysis)](https://ssd.eff.org/en/glossary/risk-analysis) being broken when someone else can obtain (or guess) those pieces of information. Services that offer [two-factor authentication[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/two-factor-authentication)](https://ssd.eff.org/en/glossary/two-factor-authentication) also require to provide a separate confirmation that you are who you say you are. The second factor could be a one-off secret code, a number generated by a program running on a mobile device, or a device that you carry and that you can use to confirm who you are. Companies like banks, and major internet services like Google, Paypal and Twitter now offer two-factor authentication.

[**Virtual Private Network**](https://ssd.eff.org/en/glossary/virtual-private-network)

A [virtual private network[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/virtual-private-network)](https://ssd.eff.org/en/glossary/virtual-private-network) is a method for connecting your computer securely to the network of an organization on the other side of the Internet. When you use a [VPN[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/virtual-private-network)](https://ssd.eff.org/en/glossary/virtual-private-network), all of your computer's Internet communications is packaged together, encrypted and then relayed to this other organization, where it is decrypted, unpacked, and then sent on to its destination. To the organization's network, or any other computer on the wider Internet, it looks like your computer's request is coming from inside the organization, not from your location.

VPNs are used by businesses to provide secure access to internal resources (like file servers or printers). They are also used by individuals to bypass local censorship, or defeat local surveillance.

[**Voice over IP (VoIP)**](https://ssd.eff.org/en/glossary/voice-over-ip-voip)

Any technology that allows you to use the Internet for voice communication with other [VoIP[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/voice-over-ip-voip)](https://ssd.eff.org/en/glossary/voice-over-ip-voip) users or receive telephone calls over the Internet.

[**Web browser**](https://ssd.eff.org/en/glossary/web-browser)

The program you use to view web sites. Firefox, Safari, Internet Explorer and Chrome are all web browsers. Smartphones have a built-in [web browser[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/web-browser)](https://ssd.eff.org/en/glossary/web-browser) app for the same purpose.

[**Web-based proxy**](https://ssd.eff.org/en/glossary/web-based-proxy)

A website that lets its users access other, blocked or censored websites. Generally, the web proxy will let you type a web address (or URL) onto a web page, and then redisplay that web address on the proxy page. Easier to use than most other censorship-circumventing services.

[**XMPP**](https://ssd.eff.org/en/glossary/xmpp)

A open standard for instant messages - Google uses [XMPP[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/xmpp)](https://ssd.eff.org/en/glossary/xmpp) for Google Chat; Facebook used to offer it, but stopped. Non-corporate independent instant messaging services will usually use XMPP. Services like WhatsApp have their own, closed and secret [protocol[https://ssd.eff.org/sites/all/themes/ssd/img/info.png](https://ssd.eff.org/en/glossary/protocol)](https://ssd.eff.org/en/glossary/protocol).

[**Zero day**](https://ssd.eff.org/en/glossary/zero-day)

A flaw in a piece of software or hardware that was previously unknown to the maker of the product. Until the manufacturers hear of the flaw and fix it, attackers can use it for their own purposes.

**Security in a box Glossary**

Some of the technical terms that you will encounter, as you read through Umbrella’s lessons, are defined below:

* ***Android***: A Linux-based open-source operating system for smartphones and tablet devices, developed by Google.
* ***APG***: Android Privacy Guard: FOSS app for Android smartphones which facilitates OpenPGP encryption. It can be integrated with K9 Mail.
* ***.apk file***: The file extension used for Android apps.
* ***App Store***: The default repository from which iPhone applications can be found and downloaded.
* ***Avast*** - A freeware anti-virus tool
* ***Basic Input/Output System (BIOS)*** - The first and deepest level of software on a computer. The BIOS allows you to set many advanced preferences related to the computer's hardware, including a start-up password
* ***BlackBerry***: A brand of smartphones which run the BlackBerry operating system developed by Research In Motion (RIM).
* ***Blacklist*** - A list of blocked websites and other Internet services that can not be accessed due to a restrictive filtering policy
* ***Bluetooth*** - A physical wireless communications standard for exchanging data over short distances from fixed and mobile devices. Bluetooth uses short wavelength radio transmissions.
* ***Booting*** - The act of starting up a computer
* ***CCleaner*** - A freeware tool that removes temporary files and potentially sensitive traces left on your hard drive by programs that you have used recently and by the Windows operating system itself
* ***CD Burner*** - A computer CD-ROM drive that can write data on blank CDs. *DVD burners* can do the same with blank DVDs. *CD-RW \*and \*DVD-RW drives* can delete and rewrite information more than once on the same CD-RW or DVD-RW disc.
* ***Circumvention*** - The act of bypassing Internet filters to access blocked websites and other Internet services
* ***Clam Win*** - A FOSS Anti-virus program for Windows
* ***Cobian Backup*** - A FOSS backup tool. The most recent version of Cobian is closed-source freeware, but prior versions are released as FOSS.
* ***Comodo Firewall*** - A freeware firewall tool
* ***Cookie*** - A small file, saved on your computer by your browser, that can be used to store information for, or identify you to, a particular website
* ***Cryptonite***: A FOSS app for file encryption on Android smartphones.
* ***Digital signature*** - A way of using encryption to prove that a particular file or message was truly sent by the person who claims to have sent it
* ***Domain name*** - The address, in words, of a website or Internet service; for example: www.securityinabox.org
* ***EDGE, GPRS, UMTS***: Enhanced Data Rates for GSM Evolution, General Packet Radio Service, and Universal Mobile Telecommunications System – technologies which allow mobile devices to connect to the internet.
* ***Encryption*** - A way of using clever mathematics to *encrypt*, or scramble, information so that it can only be *decrypted* and read by someone who has a particular piece of information, such as a password or an *encryption key*
* ***Enigmail*** - An add-on for the Thunderbird email program that allows it to send and receive encrypted and digitally signed email
* ***Eraser*** - A tool that securely and permanently deletes information from your computer or removable storage device
* ***F-Droid***: An alternative repository from which many FOSS Android applications can be found and downloaded.
* ***Firefox*** - A popular FOSS Web browser that provides an alternative to Microsoft Internet Explorer
* ***Firewall*** - A tool that protects your computer from untrusted connections to or from local networks and the Internet
* ***Free and Open Source Software (FOSS)*** - This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it
* ***Freeware*** - Includes software that is free of charge but subject to legal or technical restrictions that prevent users from accessing the source code used to create it
* ***Gibberbot***: A FOSS app for Android which facilitates secure chats over XMPP protocol (used also by Google Talk). It is compatible with Off-the-Record and, when used in conjunction with Orbot, can route chats through the Tor network.
* ***Google Play***: The default repository from which Android applications can be found and downloaded.
* ***GNU/Linux*** - A FOSS operating system that provides an alternative to Microsoft Windows
* ***Global Positioning System (GPS)*** - A space-based global navigation satellite system that provides location and time information in all weather, anywhere on or near the Earth, where there is an (almost) unobstructed sky view.
* ***Guardian Project***: An organisation which creates smartphone apps, mobile devices operating system enhancements and customisations with privacy and security in mind.
* ***Hacker*** - In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely
* ***iPhone***: A brand of smartphones designed by Apple which run the Apple's iOS operating system.
* ***Internet Protocol address (IP address)*** - A unique identifier assigned to your computer when it is connected to the Internet
* ***Internet Service Provider (ISP)*** - The company or organisation that provides your initial link to the Internet. The governments of many countries exert control over the Internet, using means such as filtering and surveillance, through the ISPs that operate in those countries.
* ***Infrared Data Association (IrDA)*** - A physical wireless communications standard for the short-range exchange of data using infrared spectrum light. IrDA is replaced by Bluetooth in modern devices.
* ***Java Applications (Applets)*** - Small programs that can run under many operating systems, are cross-platform. They are frequently used to provide improved functionalities within web pages.
* ***Jailbreaking***: The process of unlocking features on an iPhone which are otherwise blocked by the manufacturer or mobile carrier in order to gain full access to the operating system.
* ***K9 Mail***: A FOSS e-mail client for Android smartphones, which enables OpenPGP encryption when used with the APG app.
* ***Keylogger*** - A type of spyware that records which keys you have typed on your computer's keyboard and sends this information to a third party. Keyloggers are frequently used to steal email and other passwords.
* ***KeePass*** - A freeware secure password database
* ***LiveCD*** - A CD that allows your computer to run a different operating system temporarily.
* ***Malware*** - A general term for all malicious software, including *viruses*, *spyware*, *trojans*, and other such threats
* ***Mnemonic device*** - A simple trick that can help you remember complex passwords
* ***NoScript*** - A security add-on for the Firefox browser that protects you from malicious programs that might be present in unfamiliar webpages
* ***Obscuracam***: A FOSS app for Android smartphones, which protects identity of people by facilitating editions such as face-blurring to photographs.
* ***Orbot***: A FOSS app for Android smartphones which enables apps such as Orweb and Gibberbot to connect to the Tor network.
* ***Orweb***: A FOSS web browser for Android smartphones which, when used in conjunction with Orbot, facilitates browsing over the Tor network.
* ***Off the Record (OTR)*** - An encryption plugin for the Pidgin instant messaging program
* ***Peacefire*** - Subscribers to this free service receive periodical emails containing an updated list of circumvention proxies, which can be used to bypass Internet censorship
* ***Physical threat*** - In this context, any threat to your sensitive information that results from other people having direct physical access your computer hardware or from other physical risks, such as breakage, accidents or natural disasters
* ***Pidgin*** - A FOSS instant messaging tool that supports an encryption plugin called *Off the Record (OTR)*
* ***Proxy*** - An intermediary service through which you can channel some or all of your Internet communication and that can be used to bypass Internet censorship. A proxy may be public, or you may need to log in with a username and password to access it. Only some proxies are secure, which means that they use encryption to protect the privacy of the information that passes between your computer and the Internet services to which you connect through the proxy.
* ***Proprietary software*** - The opposite of Free and Open-Source Software (*FOSS*). These applications are usually commercial, but can also be *freeware* with restrictive license requirements.
* ***RiseUp*** - A email service run by and for activists that can be accessed securely either through webmail or using an email client such as *Mozilla Thunderbird*
* ***Rooting***: The process of unlocking features on an Android Phone which are otherwise blocked by the manufacturer or mobile carrier in order to gain full access to the operating system.
* ***Router*** - A piece of networking equipment through which computers connect to their local networks and through which various local networks access the Internet. *Switches*, *gateways* and *hubs* perform similar tasks, as do wireless *access points*for computers that are properly equipped to use them
* ***Secure password database*** - A tool that can encrypt and store your passwords using a single master password
* ***Secure Sockets Layer (SSL)*** - The technology that permits you to maintain a secure, *encrypted* connection between your computer and some of the websites and Internet services that you visit. When you are connected to a website through SSL, the address of the website will begin with ***HTTPS*** rather than ***HTTP***.
* ***Security certificate*** - A way for secure websites and other Internet services to prove, using encryption, that they are who they claim to be. In order for your browser to accept a *security certificate* as valid, however, the service must pay for a*digital signature* from a trusted organization. Because this costs money that some service operators are unwilling or unable to spend, however, you will occasionally see a *security certificate* error even when visiting a valid service.
* ***Security policy*** - A written document that describes how your organization can best protect itself from various threats, including a list of steps to be taken should certain security-related events take place
* ***Security cable*** - A locking cable that can be used to secure a laptop or other piece of hardware, including external hard drives and some desktop computers, to a wall or a desk in order to prevent it from being physically removed
* ***Server*** - A computer that remains on and connected to the Internet in order to provide some service, such as hosting a webpage or sending and receiving email, to other computers
* ***SIM card*** - A small, removable card that can be inserted into a mobile phone in order to provide service with a particular mobile phone company. SIM cards can also store phone numbers and text messages.
* ***Skype*** - A freeware Voice over IP (VoIP) tool that allows you to speak with other Skype users for free and to call telephones for a fee. The company that maintains Skype claims that conversations with other Skype users are encrypted. Because it is a closed-source tool, there is no way to verify this claim, but many people believe it to be true. Skype also supports instant messaging.
* ***Source code*** - The underlying code, written by computer programmers, that allows software to be created. The source code for a given tool will reveal how it works and whether it may be insecure or malicious.
* ***Spybot*** - A freeware anti-malware tool that scans for, removes and helps protect your computer from spyware
* ***Steganography*** - Any method of disguising sensitive information so that it appears to be something else, in order to avoid drawing unwanted attention to it
* ***Swap file*** - A file on your computer to which information, some of which may be sensitive, is occasionally saved in order to improve performance
* ***Textsecure***: A FOSS app for Android which facilitates encrypted sending and storage of text messages.
* ***Thunderbird*** - A FOSS email program with a number of security features, including support for the Enigmail encryption add-on
* ***Tor*** - An anonymity tool that allows you to bypass Internet censorship and hide the websites and Internet services you vist from anyone who may be monitoring your Internet connection, while also disguising your own location from those websites
* ***TrueCrypt*** - A FOSS file encryption tool that allows you to store sensitive information securely
* ***Undelete Plus*** - A freeware tool that can sometimes restore information that you may have deleted accidentally
* ***Uninterruptable Power Supply (UPS)*** - A piece of equipment that allows your critical computing hardware to continue operating, or to shut down gracefully, in the event of a brief loss of power
* ***VautletSuite 2 Go*** - A Freeware encrypted email program
* ***Voice over IP (VoIP)*** - The technology that allows you to use the Internet for voice communication with other VoIP users and telephones
* ***Whitelist*** - A list of websites or Internet services to which some form of access is permitted, when other sites are automatically blocked
* ***Windows Phone***: A smartphone operating system developed by Microsoft.
* ***Wiping*** - The process of deleting information securely and permanently
* ***Your-Freedom*** - A freeware circumvention tool that allows you to bypass filtering by connecting to the Internet through a private proxy. If Your-Freedom is configured properly, your connection to these proxies will be encrypted in order to protect the privacy of your communication.