

MISA ZIMBABWE



DIGITAL SECURITY GUIDE



INTRODUCTION

This Digital Security guide is produced by the Media Institute of Southern Africa – Zimbabwe Chapter [MISA-Zimbabwe], as part of its Broadcasting and Information, Communication Technologies (ICT) programme.

As an organisation that advocates freedom of expression through diverse and free communication platforms, MISA-Zimbabwe recognises the internet as a critical platform for Zimbabweans to share information and access information. Zimbabwe's media space remains highly constricted owing to a number of challenges that include the legislative environment and the economic decline in the country.

This leaves the internet as an alternative platform- particularly with the rise in internet penetration in the country over the past decade.

While access to the internet has also implied that new communication technologies such as mobile phones, tablets and laptops are relatively cheaper and even more-user friendly, they have also become more difficult to understand, particularly when it comes to issues of security and privacy. There are also concerns about who owns data when it is created and published online. These concerns are even greater for the media, particularly when

looking at whether individuals can control and protect, with the basic default privacy settings, footprints of sensitive information and sources.

MISA-Zimbabwe through this manual, is encouraging and urging media practitioners – mainstream and citizen journalists - as well as online producers of content, to secure their communication while they exercise their rights and responsibilities of producing news content without falling foul of the law.

Compiled by CNM Technologies for MISA Zimbabwe

With some information from www.securityinabox.org ;Microsoft Windows support; Facebook support; Twitter support; Google chrome; Firefox browser.

CONTENTS

| | |
|--|-----------|
| Why secure | 1 |
| Physical security related risks | 1 |
| Software related risks | 2 |
| Computer Basics | 2 |
| To deal with malware you need a good antivirus programme | 2 |
| How to choose an antivirus programme | 4 |
| Firewall | 4 |
| Keeping your software up to date | 5 |
| Pirated software should never be used | 6 |
| Passwords | 7 |
| How to set a password on your windows computer | 9 |
| Change password | 10 |
| Auto-Lock your computer when its idle | 10 |
| Online security | 11 |
| Securing your Internet browser | 11 |
| Tips for Secure Browsing with Google Chrome | 12 |
| Tips for Secure Browsing with Mozilla Firefox | 12 |
| Private browsing | 13 |
| In Chrome | 14 |
| Gmail security | 15 |
| Security on social networks | 19 |
| Facebook security and privacy settings | 19 |
| Twitter | 22 |
| YouTube | 22 |
| Mobile phone security | 23 |
| Physical security for your mobile phone | 23 |
| BASIC FUNCTIONS, TRACKABILITY AND ANONYMITY | 24 |
| About eavesdropping | 24 |
| About interception of calls | 25 |
| SECURITY SETTINGS FOR ANDROID SMARTPHONE | 25 |
| DEVICE ENCRYPTION | 25 |
| NETWORK SETTINGS | 25 |
| CALLER IDENTITY | 26 |
| APPS FOR ANDROID | 26 |
| Digital Security Terminology | 29 |

Why Secure

Every day, everywhere, digital technology is generating new possibilities; new ways to work and play, to transact and interact. Our work, play, and personal lives revolve around computers, internet and mobile phones.

The benefits of technology are obvious – but there are security implications too. Potentially, the more we use technology, the more the number of security risks for organisational and personal information. From bank accounts to personal photos and messages, we all have data stored on digital devices and online accounts—and also more to lose. All our private conversations are out there somewhere. But for those who were born with an iPad in their hands, “digital security” might as well be a foreign language.

There are usually three technology related risks you might think about:

Information or Data Loss.

When your hard drive dies, your computer is affected by a power surge, your phone gets smashed, or you lose your camera's data card, or even water or fire damage.

When affected by malware (malicious software). Some viruses can destroy data on your computer or mobile device

When you forget your password.

Disclosure. Someone (or some people), learns something that you would prefer to keep private.

When your computer mobile device, flash disk, or SIM card is lost

When someone gets hold of your password to your computer service like email, cloud storage (like drop box, Google drive)

Interruption. Your network connection stops working, you can't send an email, or your phone doesn't have a signal.

When your hard drive dies, your computer is affected by Power surge, your phone gets smashed, or you lose your camera's data card, or even water or fire damage.

When affected by malware (malicious software). Some viruses can destroy data on your computer or mobile device.

When you forget your password.

Physical security related risks:

As we read in newspapers every day, the chances that your phone or laptop gets stolen are uncomfortably high. So what would happen if your mobile device falls into the wrong hands? Before we talk about the different tips and tricks to secure your computer or mobile device, keeping your device safe is the first step towards digital security.

Many people love to say that a stolen device occurrence is a one-off mishap, while for some, it is something that never happens.

Here is what happened to Coca Cola, one of the largest and most recognised brands in the world and employer of over 700 000 people. You would think that keeping the details and information of its employees and customers would be of paramount importance, so much so that only an Ocean's 11 style heist would be able to pry such sensitive data from their grasp. Unfortunately, it seems as though a simple theft of a few unencrypted laptops resulted in the loss of sensitive information for around 74 000 North American-based employees.

Source: <http://www.bloomberg.com/news/articles/2014-01-24/coca-co-la-says-74-000-affected-after-company-laptops-stolen>

Do you know where your computer or mobile device is?

Do you know where and what we put on that USB sticks?

Software related Risks

Malware (for "malicious software")

This is any programme or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, programming that gathers information about a computer user without permission.

Viruses

There are many different ways to classify viruses, and each of these methods comes with its own set of colourfully-named categories. Worms, Macro viruses, Trojans and backdoors, are some of the more well-known examples. Several of these viruses spread over the Internet, using email, malicious web pages or other means to infect unprotected computers.

Others spread through removable media, particularly devices like USB memory sticks and external hard drives that allow users to write information as well as reading it. Viruses can destroy, damage or infect the information in your computer, including data on external drives. They can also take control of your computer and use it to attack other computers. Fortunately there are many anti-virus tools that you can use to protect yourself and those with whom you exchange digital information.

Spyware

Spyware is a class of malicious software that can track the work you do, both on your computer and on the Internet, and send information about it to someone who shouldn't have access to it. These programmes can record the words you type on your keyboard, the movements of your mouse, the pages you visit and the programmes you run, among other things. As a result, they can undermine your computer's security and reveal confidential information about you, your activities and your contacts. Computers become infected with spyware in much the same way that they contract viruses. The suggestions above are also helpful when defending against this second class of malware. Because malicious web pages are a major source of spyware infection, you should pay extra attention to the websites you visit and make sure that your browser settings are secure.

Computer Basics

Keeping your device healthy is a critical step towards digital security. So, before you begin worrying too much about strong passwords, private communication and secure deletion, for example, you need to make sure that your computer is not vulnerable to hackers or plagued by malicious software, malware.

Otherwise, it is impossible to guarantee the effectiveness of any other security precautions you might take.

After-all, there is no point in locking your door if the burglar is already downstairs, and it doesn't do you much good to search downstairs if you leave the door wide open.

To deal with malware you need a good antivirus program

Antivirus software is used to safeguard a computer from malware, including viruses, computer worms, and Trojan horses. Antivirus software may also remove or prevent spyware and adware, along with other forms of malicious programmes.

By installing anti-virus software, you can prevent your computer from getting viruses and other malware.

Do you already have it installed?

The best way to tell if you have anti-virus software installed is to use the Security Centre feature on your Microsoft operating system. When you select this option, you will be presented with a status for:

- Anti-virus software.
- Firewall protection.

You can do this by following these simple steps:

If your computer is running Windows 8

If your computer is running Windows 8, you already have antivirus software. Windows 8 includes, Windows Defender, which helps protect you from viruses, spyware, and other malicious software.

If Windows Defender is turned off and you don't have another antivirus programme installed [or your other antivirus programme is not working], you will see a warning in the notification area on your taskbar.

If your computer is running Windows 7

Windows 7 includes spyware protection, but to protect against viruses you can download Microsoft Security Essentials for free.

To find out if you already have antivirus software:

- Open Action Center by clicking the Start button, clicking Control Panel, and then, under System and Security, clicking Review your computer's status.
- Click the arrow button next to Security to expand the section.

If Windows can detect your antivirus software, it's listed under Virus protection.

Windows doesn't detect all antivirus software, and some antivirus software don't report their status to Windows. If your antivirus software isn't displayed in Action Center and you're not sure how to find it, try any of the following:

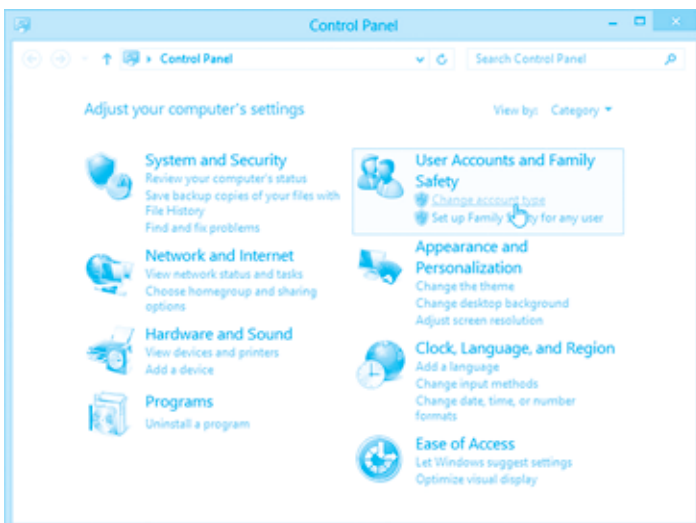
- Type the name of the software or the publisher in the Search box on the Start menu.
- Look for your antivirus programme icon in the notification area of the taskbar

If Windows can detect your antivirus software, it will be listed under Virus protection.

Windows does not detect all antivirus software, and some antivirus software don't report their status to Windows.

If your antivirus software is not displayed in Windows Security Center and you're not sure how to find it, try any of the following:

- Look for the antivirus software in the list of programmes on the Start menu.
- Type the name of the software or the publisher in the Search box on the Start menu.
- Look for the icon in the notification area of the taskbar.





How to choose an antivirus programme

You know you need antivirus, but with so many from which to choose, how do you know which antivirus software is best?

The major certification and testing agencies and websites to see how the antivirus scanners fare include:

- VB100% : <http://www.virusbtn.com/vb100/index>,
- Checkmark, : <http://www.westcoastlabs.com/checkmark/>
- ICسا Labs: <https://www.icsalabs.com/products>
- AV-Test: <http://www.av-test.org/>
- AV-Comparatives, <http://www.av-comparatives.org/>

Any antivirus scanner worth consideration should be listed by most of these antivirus testing agencies.

Firewall

A good firewall allows you to choose access permissions for each programme on your computer. When one of these programmes tries to contact the outside world, your firewall will block the attempt and give you a warning unless it recognises the programme and verifies that you have given it permission to make that sort of connection. This is largely to prevent existing malware from spreading viruses or inviting hackers into your computer. In this regard, a firewall provides both a second line of defence and an early-warning system that might help you recognise when your computer's security is being threatened.

Recent versions of Microsoft Windows include a built-in firewall, which is now turned on automatically.

Take the following steps to turn on windows firewall:

- Open Windows Firewall by clicking the **Start** button, and then clicking **Control Panel**. In the search box, type **firewall**, and then click **Windows Firewall**.
- In the left pane, click **Turn Windows Firewall on or off**. If you're prompted for an administrator

password or confirmation, type the password or provide confirmation.



Turn Windows Firewall on or off link in Windows Firewall

- Click **Turn on Windows Firewall** under each network location that you want to help protect, and then click OK.
- If you want the firewall to prevent all programs from communicating, including programmes that you have previously allowed to communicate through the firewall, select the **Block all incoming connections**, including those in the list of allowed programs check box.

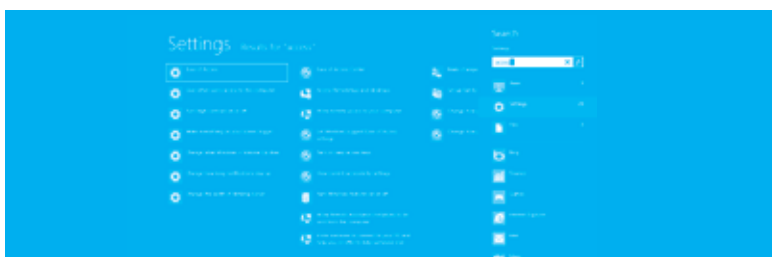
Keeping your software up-to date

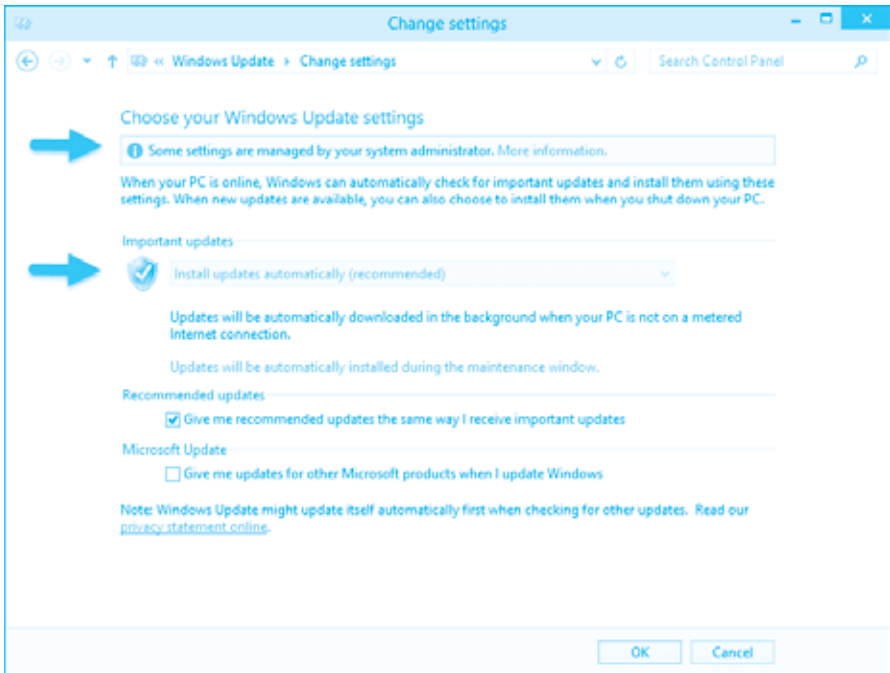
Computer programmes are often large and complex. It is inevitable that some of the software you use on a regular basis contains undiscovered errors, and it is likely that some of these errors could undermine your computer's security. Software developers continue to find these errors, however, and release updates to fix them. It is therefore essential that you frequently update all of the software on your computer, including the operating system.

To have Windows install important updates as they become available, turn on automatic updating. Important updates provide significant benefits, such as improved security and reliability. You can also set Windows to automatically install recommended updates, which can address non-critical problems and help enhance your computing experience. Optional updates and Microsoft updates aren't downloaded or installed automatically.

Open Windows Update by swiping in from the right edge of the screen. If you are using a mouse, point to the lower-right corner of the screen and moving the mouse pointer up, tapping or clicking **Settings**, tapping or clicking **Change PC settings**, and then tapping or clicking **Update and recovery**.

- Tap or click **Choose how updates get installed**.
- Under **Important updates**, choose the option that you want.
- Under **Recommended updates**, select the **Give me recommended updates the same way I receive important updates** check box.
- Under **Microsoft Update**, select the **Give me updates for other Microsoft products when I update Windows** check box, and then tap or click Apply.





How much does it cost to update Windows automatically?

Windows Update is free. However, depending on how you are billed for your Internet connection, by your Internet service charges (eg. your ISP Econet bundles, ZOL, Powertel), or mobile data charges might apply for the time required to download an update. Best time to schedule the updates is when you are at work or where there is a WiFi connection with uncapped bandwidth.

Turn on automatic app updates : Applies to Windows 8.1, Windows RT 8.1

App publishers sometimes update their apps to add new features and fix problems. The Windows Store can automatically install app updates when they become available.

To make sure your apps get updated automatically, follow these steps:

- On the **Start screen**, tap or click **Store** to open the **Windows Store**.
- Swipe in from the right edge of the screen, and then tap **Settings**. [If you're using a mouse, point to the lower-right corner of the screen, move the mouse pointer up, and then click Settings.]
- Tap or click **App updates**.
- Make sure your **Automatically update my apps** is set to **Yes**.

If your computer is running Windows XP

On April 8, 2014, Microsoft ended support for Windows XP. This means that there are no new security updates available through automatic updating for computers that are still running Windows XP.

Pirated software should never be used

Software prices are quite high for the ordinary Zimbabwean so many users turn to installing bootleg copies, or pirated ones. You may encounter many risks if using pirated software.

The first risk that you run is infecting your PC with malware. The crack might actually be a disguised malware.

Malware as mentioned before is malicious software and does some damage like – slowing your PC down, sending out your information. This includes credit card and bank account numbers, passwords and address books, all of which can be immediately exploited by identity thieves.

The second risk is the program not actually working. Most software companies have implemented a way of checking the registration – the program might work for a while, but receive an update at some point in time which renders it unusable unless you make a purchase. Some might disable the Automatic Update feature of the software in question. This comes with a downside, though: no vulnerability patches for you, as the developers often push them through a product update.

Passwords

Your password is what tells the computer or service that you are who you say you are. Until we can do retina scans like in James Bond movies, the password is the best that we can do. But, because your password is like a key to your account, you need to safeguard it. Anyone who has your password can get into your account, and your files. Anyone who can guess your password has it. Anyone who has your password can pose as you. Therefore, you may be held responsible for someone else's actions, if they are able to get your password. You may not wish this to happen. Today you need to remember many passwords. You need a password for the Windows log on, your e-mail account, Facebook, Twitter, Ecocash or Telecash, the list is just endless.

A weak password:

- Contains less than eight characters.
- Is a word found in a dictionary (English or foreign).
- Is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software, sports teams (Dembare or Highlanders).
- Birthdays and other personal information such as addresses, phone numbers, or license plates.
- Word or number patterns like aaabbb, qwerty, 9876543.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (harare52).

Strong passwords

Use longer, varied passwords

A rule of thumb for strong passwords is the longer, the better. Passwords that have a greater number of varied characters is more difficult for hackers to crack. Many websites require accounts to have six or more characters. However, users that go above and beyond these guidelines are at a reduced risk of infiltration. In addition, individuals should seek to include numbers, symbols and other characters where allowed.

Another rule of thumb, avoid biological or personal details in passwords. Eg. your birth-date or child's name.

Don't use things that is specifically about you, such as your hometown or the name of your pet or spouse."

Passwords are hacked or cracked in the following ways:

- **A dictionary attack** is a method of breaking into a password-protected computer or service by systematically entering every word in a dictionary as a password. So if your password is a dictionary word then it can be cracked this way.
- **Bruteforce attack** involves trying every key combination until the correct password is found. Due to the number of possible combinations of letters, numbers, and symbols, a brute force attack can take a long time to complete.

What not to do when choosing a password

- Do **not** choose a password based upon personal data like your name, your username, or other

information that one could easily discover about you from such sources as searching the internet.

- Do **not** choose a password that is a word (English or otherwise), proper name, name of a TV show, keyboard sequence, or anything else that one would expect a clever person to put in a "dictionary" of passwords.
- Do **not** choose a password that is a simple transformation of a word, such as putting a punctuation mark at the beginning or end of a word, converting the letter "l" to the digit "1", writing a word backwards, etc. For example, "password, 123" is not a good password, since adding ",123" is a common, simple transformation of a word.
- Do **not** choose passwords less than 8 characters long or that are made up solely of numbers or letters. Use letters of different cases, mixtures of digits and letters, and/or non-alphanumeric characters.

Methods for choosing passwords

The single best method for generating passwords is to do the following:

1. Make up a sentence you can easily remember. Some examples:
I have two kids: Jack and Jill.
I like to eat Dave & Andy's ice cream.
No, the capital of Wisconsin isn't Cheeseopolis!
2. Now take the first letter of every word in the sentence, and include the punctuation. You can throw in extrapunctuation, or turn numbers into digits for variety. The above sentences would become:
Ih2k:JaJ.
IlteD&A'ic.
N,tcoWiCl

As you can see, the passwords generated by this method can be fairly secure, but are easy to remember if the sentence you pick is one that is easy for you to remember. In cases where an application allows long passwords, you could possibly use the entire phrase as your "password".

Please don't use one of the sentences above to generate your password.

Another password selection method

If you don't wish to use the above method, the following method also generates "reasonably secure" passwords (though not quite as good as the method above) that may be easier to remember:

1. Choose two or more unrelated words such as:
 - unix & fun
 - book & goat
 - august & brick
2. Join the words with a non-alphabetic character or two.
3. Make at least one change (for example, uppercase a letter or add another character) to one or more of the words (preferably not just at the very beginning or end of the password).

Some example passwords generated using this method:

- unix+PhUn
- bolok29goat
- august.=bRICK

Please don't use one of the passwords above.

How long should be my password?

In general, the longer a password is, the harder it is for somebody to guess or brute-force it. Password selection trades off security with convenience and the ability to remember it. **Eight characters should be the absolute minimum length.** SCS Kerberos passwords may of practically unlimited length (the limit is at least several hundred characters). Windows 2000 and Windows XP support a maximum password length of 127 characters. There are a few cases where you might run into password length limitations:

- Some older Unix systems may only support passwords up to 8 characters, or ignore any letters after the first 8. This should not be a limitation if you login with your Kerberos password to Facilitized SCS hosts.
- Some applications for reading e-mail via POP may have trouble with long (greater than 8 character) passwords. This should only affect your choice of a .mail Kerberos instance password, not your main

Kerberos password.

- Windows 98 and 95 only support passwords up to 14 characters long.

In a Windows environment, there are certain security advantages to be gained if your password is 15 characters or longer.

Can I write my password down?

You should avoid writing down your password or giving it to others. You should especially avoid writing it down and leaving it in a non-secured place such as on a post-it on your monitor or a piece of paper in your desk. If you absolutely must write something down, we suggest doing the following:

- Don't write down the entire password, but rather a hint that would allow you (but nobody else) to reconstruct it.
- Keep whatever is written down in your wallet or other place that only you have access to and where you would immediately notice if it was missing or someone else gained access to it.

Why is this important?

It is very common for intruders to attempt to break-in to systems (both Unix and Windows) at SCS by trying to guess people's passwords. Sometimes they succeed, and when they do it is often because people chose very poor passwords (like "password" or "administrator"). These break-ins can result in a significant amount of downtime, lost work, and loss of privacy (for example, if there is credit card and other financial data on your machine). Intruders often also install keyboard sniffers that let them gather additional passwords and put more machines at risk. They can also conduct dictionary attacks against a host's password database, and literally try out tens of thousands of potential passwords per second, which is why words and simple variants of words are not good passwords.

How to set a password on your windows computer

1. Open User Accounts by clicking the **Start** button  clicking **Control Panel**, clicking **User Accounts** and **Family Safety**, and then clicking **User Accounts**.

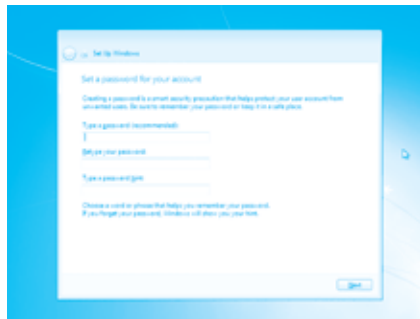
2. Click **Create a password**.

If there's already a password for this user account, you can change it by clicking **Change your password**.

3. Type the password in the **New password** box, and then type the password again in the **Confirm new password** box.

4. If you would like to use a password hint, type the hint in the **Password hint** box.

5. Click **Create password**.



Changing your Windows password on a regular basis is a good habit to help keep your PC secure. You might also want to change your Windows 7 password if you have been having problems remembering or entering

Change password

your current one.

Changing your password in Windows 7 is very easy. Follow the easy steps below to change your Windows 7 password:

1. Press CTRL+ALT+DELETE, and then click Change password.
2. Type your old password, type your new password, type your new password again to confirm it, and then press ENTER.

Auto-Lock your computer when its idle

You can help make your computer more secure by creating a screen saver password, which locks your computer when the screen saver is on. The screen saver password is the same password that you use to log on to Windows.

1. Open **Screen Saver Settings** by clicking the **Start button** and then clicking **Control Panel**. In the **Search Box**, type screen saver, and then click Set screen saver password.
2. Select the On resume, display logon screen check box, set a time when you want the screen saver to start, and then click OK. (Choose a time that's not long enough for an unauthorized person to use your computer, but not so short that if you stop working at your computer for a moment, the screen saver locks it.)



You can also lock your computer by using the **Ctrl+Alt+Delete** keyboard combination and then selecting **Lock screen**.

You can also simply use the Windows+L keyboard combination to automatically lock the screen. Your computer will require a password to unlock it.



Online security

The Internet offers so many opportunities to explore, create and collaborate. And to make the most of the web, is important to keep yourself safe and secure. Whether you are a new Internet user or an expert, the advice and tools here can help you navigate the web safely and securely.

Securing your Internet browser

An internet browser is the programme that you use to access the internet and view web pages on your computer. Some common internet browser examples include:

- Internet Explorer
- Mozilla Firefox
- Safari
- Chrome

Optimising your browser's settings is a critical step in using the Internet securely and privately. Today's popular browsers include built-in security features, but users often fail to optimize their browser's security settings on installation. Failing to correctly set up your browser's security features can put you at a higher risk for malware infections and malicious attacks.

1. Keep your browser updated

Frequently, browser updates are released to plug recently discovered security holes. So it's important to always keep any browsers you use updated.

2. Be cautious when installing plug-ins

Plug-ins and extensions can sometimes put you at risk. For instance, at the beginning of 2015, it was discovered that some Chrome extensions can change service or ownership without notification to users. As a result, Chrome's regulations for extensions changed in June 2015 to keep extensions from becoming anything other than "simple and single-purpose in nature," according to Google.

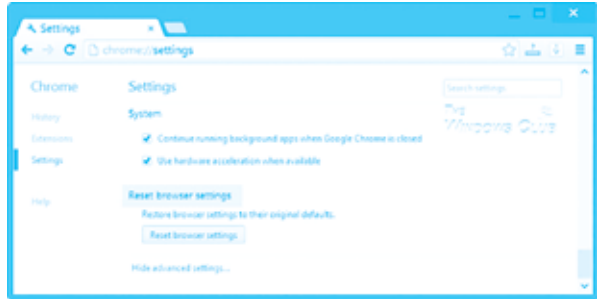
3. Install security plug-ins

The majority of plug-ins and extensions are safe, however, some can help bolster your browser's security. Here are three suggested—and free—browser extensions for added security.

- **HTTPS Everywhere.** The Electronic Frontier Foundation and The Tor Project jointly developed this Firefox, Chrome, and Opera extension. HTTPS is a communications protocol for securing communications over a computer network, vs. the standard HTTP protocol, which is more widely used but less secure. (The 'S' in HTTPS stands for 'secure.') HTTPS Everywhere encrypts communication with many major websites to help secure your browsing experience.
- **Web of Trust (also known as WOT).** This extension for Internet Explorer, Firefox, Chrome, Safari, and Opera helps you determine if a website is safe to surf. The extension displays traffic signal icons next to URLs and links. Green means the site is reliable; yellow indicates you should proceed with caution; red translates to "steer clear." The ratings are crowd sourced from WOT's global user base and are supported by trusted third-party sources, such as up-to-date directories of malware sites.
- **LongURL.org.** If you are on Twitter or Facebook and you see a shortened link embedded in an interesting post, you might click it without a second thought. But shortened links have been known to mask malicious links. If you are unsure of a shortened link, copy and paste it into the search box at LongURL.org. You'll see where the link would take you, without having to actually click through to the site. LongURL.org is also available as a Firefox browser extension.

Tips for Secure Browsing with Google Chrome

These settings can be accessed through Chrome's "Advanced Settings" menu or by navigating to "chrome://settings/."



Enable phishing and malware protection: Make sure that Chrome's phishing and malware protection feature is enabled under the "Privacy" section. This feature will warn you if a site you're trying to visit may be phishing or contain malware.

Turn off instant search: The Instant search feature should be turned off for optimal security. While it offers some convenience in searching, having this feature enabled means that anything you type in the address bar is instantly sent to Google.

Don't sync: Disconnect your email account from your browser under the "Personal Stuff" tab. Syncing your email account with your Chrome browser means that personal information such as passwords, autofill data, preferences, and more is stored on Google's servers. If you must use sync, select the "Encrypt all synced data" option and create a unique passphrase for encryption.

Configure content settings: Click "Content settings" under the "Privacy" section and do the following:

- **Cookies:** Select "Keep local data only until I quit my browser" and "Block third-party cookies and site data." These options ensure that your cookies will be deleted upon quitting Chrome and that advertisers will not be able to track you using third-party cookies.
- **JavaScript:** Select "Do not allow any site to run JavaScript." It is widely recommended that JavaScript be disabled whenever possible to protect users from its security vulnerabilities.
- **Pop-ups:** Select "Do not allow any site to show pop-ups."
- **Location:** Select "Do not allow any site to track my physical location."

Configure passwords and forms settings: Disable Auto fill and deselect "Offer to save passwords I enter on the web" under the "Passwords and forms" section. Doing so will prevent Chrome from saving your logins, passwords, and other sensitive information that you enter into forms.

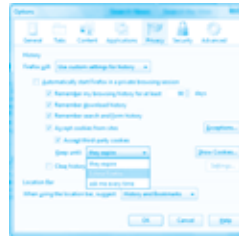
Tips for Secure Browsing with Mozilla Firefox

These settings can be accessed through the "Options" menu.



Configure privacy settings: Under the "Privacy" tab, complete the following steps. These measures ensure that Firefox is storing only as much of your information as it needs to function normally.

- Select "Use custom settings for history."
- Deselect "Remember my browsing and download history."
- Deselect "Remember search and form history."
- Deselect "Accept third-party cookies."
- Set cookie storage to "Keep until I close Firefox."
- Select "Clear history when Firefox closes."



Configure security settings: Under the "Security" tab, choose the following settings. These steps prevent Firefox from saving your passwords and keep you from visiting potentially harmful sites.

- Verify that "Warn me when sites try to install add-ons," "Block reported attack sites," and "Block reported web forgeries" are all selected.
- Deselect "Remember passwords for sites."

Disable JavaScript: Deselect "Enable JavaScript" under the "Content" tab. JavaScript is notorious for containing security vulnerabilities and it is recommended that users only enable it for trusted sites.

Enable pop-up blocking: Verify that "Block pop-up windows" is selected under the "Content" tab. This feature should be turned on by default as it protects users from unwarranted advertisements and windows.

Don't sync: Avoid using Firefox Sync. By doing so you prevent Firefox from storing your logins, passwords, and other sensitive information.

Turn on automatic updates: Verify that "Automatically install updates" is selected in the "Update" tab under "Advanced." Doing so will ensure that your browser receives critical security updates. Verify that "Automatically update Search Engines" is selected as well.

Use secure protocols: Verify that "Use SSL 3.0" and "Use TLS 1.0" are selected in the "Encryption" tab under "Advanced."

Private browsing

Private browsing is a new and important feature with browsers these days. Once you go into private browsing mode, you can browse the internet without leaving a trail. Your history? Deleted. Your cookies? Destroyed. Your bookmarks and non-private history? Preserved for when you come back to the surface.

Now, while private browsing is useful, it is not all powerful. Private browsing will not protect you from keyloggers, tracking programs, nasty viruses after your personal info, or government surveillance efforts. But as far as the average Joe is concerned, your private online activities will remain shrouded in mystery.

In Firefox

How do I open a new Private Window?

There are two ways to open a new Private Window.
Open a new, blank Private Window



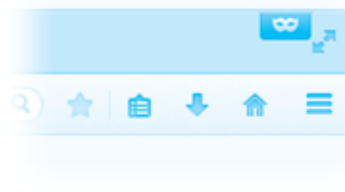
Click the menu button and then click New Private Window.

Open a link in a new Private Window


- Hold down the Ctrl key while you click on any link and choose Open Link in New Private Window from the context menu.



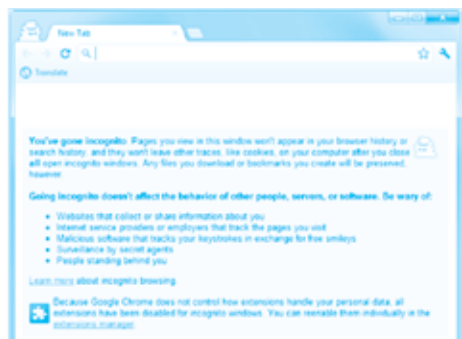
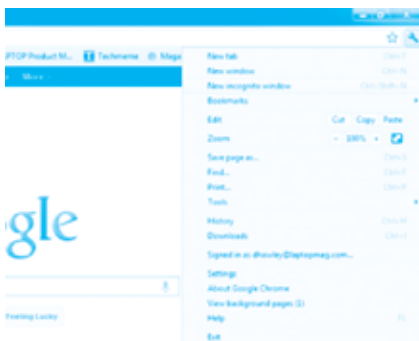
Tip: Private Browsing windows have a purple mask at the top.



In Chrome

1. Open a Chrome window
2. In the top-right corner of the browser window, click the Chrome menu .
3. Select New Incognito Window.
4. A window will open with this  in the top-right corner
5. To close incognito mode, go to the corner of each of your incognito windows and click the X.

Tip: You can also press Ctrl + Shift + N [Windows, Linux, and Chrome OS] and - Shift - N [Mac] to open an incognito window.



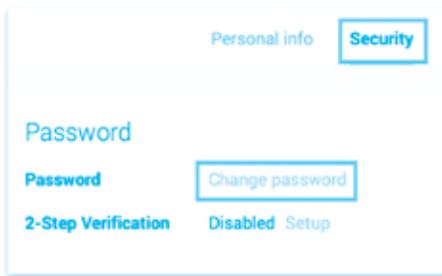
Gmail Security

Gmail is the most popular email service to date, thanks to its creator, Google, the name which is often associated with user-friendliness and security. Despite what the company does to keep your emails safe, you may still be preyed on by hackers, phishers and scammers from all over the Web.

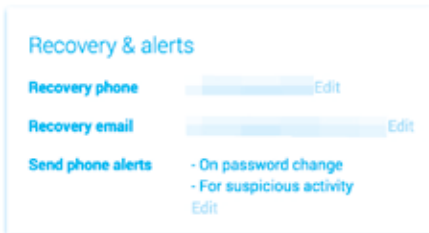
1. Protect your password

Of course, start by making sure your password is strong and **not shared**.

If you need to change it, visit the **Account Settings** page as above and click the "Security" tab. You'll find the password settings at the top of the list.



Make sure the **reset and recovery options** are safe too - in the same tab, look at the "Recovery & Alerts" section. If you've already provided Google with a phone number and/or alternate email address, they will be listed here.



Make sure they are correct, and think about whether other people may be able to get at them - if they can, they could reset your password and break into your account.

If there are no details here, you may want to think about adding some sort of recovery option in case you forget your password. These contact details are also used to send alerts when Google detects suspicious activity on your account, and the type of alerts sent can be adjusted using the "Edit" button.

Older accounts may still have a "Security question" set up. However this method of recovering an account is no longer supported and can be ignored.

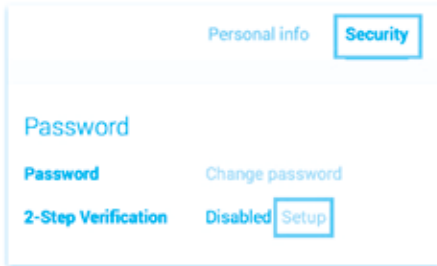
If you need help picking a good password, then our video should help:

Can't view the video on this page? Watch directly from YouTube. Can't hear the audio? Click on the Captions icon for closed captions.

2. Set up 2-step verification

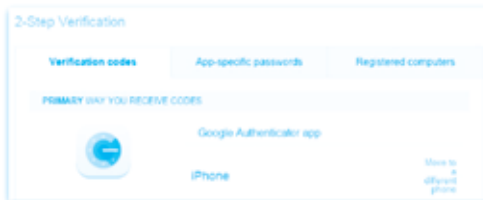
Google's version of two-factor authentication, referred to as **2-step verification** [2SV], can also be accessed from the Security tab on the Account Settings page.

You'll find it just underneath the "Change password" option.



To set it up, you will need to provide a phone number, which will be verified with an initial code sent via SMS or as an automated voice message. Click "Setup" in this section, then follow the instructions.

Note that in some regions this option is not available - possible workarounds include using one of the many services which provide free internet SMS to get the initial setup done, then switching to the **Authenticator app**.



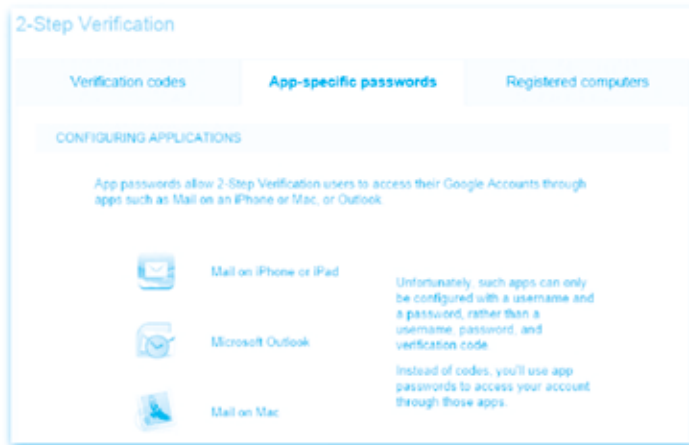
Google's app supports most phone platforms, and is useful for securing a raft of other services too. You can switch to this once the initial setup is complete, or you can stick to SMS or voice to send codes.

Once you have logged in on a given machine for the first time, Google will offer to "trust" that machine, meaning no more codes will be required - the box is checked by default, so if you log in from an untrusted system, make sure you uncheck it.

For mail client apps and other services that don't support secondary codes, you can generate a device-specific password which replaces your standard password when logging in - see the second tab in the 2SV options page.

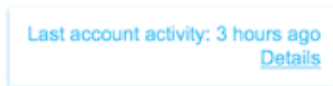
You can also provide a backup phone number, or generate a list of one-off emergency codes, to use in case of a problem with your main method of generating codes - as usual, make sure these are secure.

Google has also recently introduced its Security Key which can be plugged into your USB port and used instead of SMS or an authenticator app as your second factor of 2SV. Google's part of it is free, but you do have to pay for a compatible device. You're also restricted to Chrome when using it.



3. Check your settings

At the bottom of every page is a record of the "Last account activity", showing when you last logged on.



Click on "Details" to see the last ten logins, the IP address they originated from, and a guess at the country based on that IP address, which should be accurate in most cases.

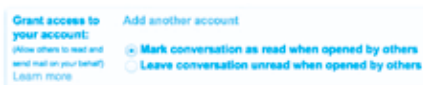
It will also show whether the access was from a browser or mobile device. For many access types you can even burrow down into each entry to find info like the browser and OS version, or mobile device type. You can also find a more detailed version of the history, complete with more precise (but still estimated) location data, on the Account Settings page under "Recent activity".

Consider checking these from time to time to look out for access from unexpected locations, and certainly look here first if you suspect someone's been intruding into your account.

If you think anyone may have had access to your account for any period of time, it's worth checking whether any **delegation** has been set up. On the main Gmail page, click the gear icon and choose "Settings".



Go to the "Accounts and import" tab and look at the "Grant access to your account" section.

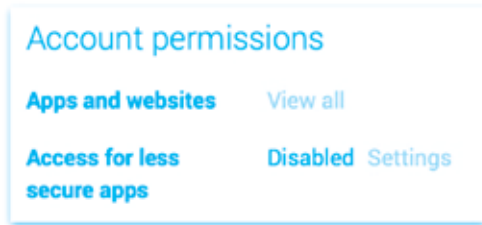


If there are any other accounts here that you have not added, those accounts could have had unfettered access to all your mail and contacts - a sneaky intruder may also have checked the "Leave conversation unread..." box, so you wouldn't be able to tell if they'd read something. Reset any unwanted changes here as soon as you spot them.

Another place to look is on the **"Filters" and "Forwarding and POP/IMAP"** tabs to check no-one's set up any rules to forward mail to a third-party address. This is less intrusive than delegated access, but can still leak a lot of stuff to someone who should not have it.



Back on the main Account Settings page (that which is reached by clicking the user ID in the top right of any Gmail page and selecting "Account") is the **"Account permissions"** section. You will find it just under the Password options.



This lists all websites and apps which have been granted access to your Google account - these might include things like mail client apps on mobile devices, or Google's own Chrome or Drive services.

Some information should be given on what each entry means - look out for things you don't need or recognise.

Check Your Filter, Forwarding and POP/IMAP

In 2007, a famous designer, David Airey's Gmail account is hijacked. To make the long story short, the hacking started when the user has its account signed on and he went to visit a bad site. The site added a backdoor to extract information from the Gmail account, and the backdoor is the Filter. Filters can potentially transfer emails as long as the victim has the filter in his account.



Therefore, it's vital for you to actually check your account settings to **delete suspicious filters**. The check is real easy. As usual, you just need to log into your Gmail account, then after clicking the gear-like icon, choose Settings >Filters to check and delete the Filter you didn't put there before.

You will also need to check the **"Forwarding and POP/IMAP"** tab as well to confirm that there is no foreign forwarding address included in this tab apart from those assigned by you. Do perform a check on these stuff when you feel that something unusual is going on in your account. Your prevention methods will save you from experiencing problems in the future.

Security on social networks

Facebook, Twitter, Google+, YouTube, Pinterest, LinkedIn and other social networks have become an integral part of online lives. Social networks are a great way to stay connected with others, but you should be wary about how much personal information you post.

A number of Zimbabweans have been arrested for various posts on social networking sites and for messages on popular whatsapp platform.

We share a wealth of information about ourselves on our social media platforms. We snap perfectly posed selfies, check in at happy hours, tweet at our friends, and announce the arrival of bouncing new babies. The benefits and joys of social media are numerous, but there are privacy risks to consider as well.

No matter which service you use, it's incumbent on you to find out where these settings live (Google is your name in that regard). Once you find them, the most important settings to look for are:

- Who can read your profile;
- Who can see your posts and activities;
- What information is shared with external sites and businesses;
- Which applications can access your data;
- What information your friends can share about you;
- Who can see your pictures and/or location;
- Which sites integrate with your social network (for example, Facebook's Like feature).

Most services allow you to control tiered privacy levels: one for friends (or immediate contacts); friends of friends (or second-degree contacts); third-parties; or everyone in the world.

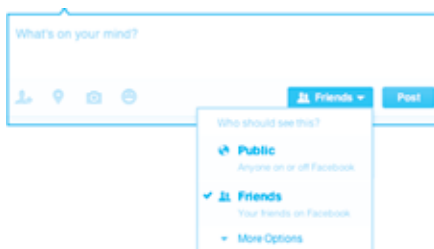
Facebook security and privacy settings

Basic Privacy Settings & Tools

Selecting an Audience for Stuff You Share

When I post something, how do I choose who can see it?

You'll find an audience selector tool most places you share status updates, photos and other things you post. Click the tool and select who you want to share something with.



The tool remembers the audience you shared with the last time you posted something and uses the same audience when you share again unless you change it. For example, if you choose Public for a post, your next post will also be Public unless you change the audience when you post. This one tool appears in multiple places, such as your privacy shortcuts and privacy settings. When you make a change to the audience selector tool in one place, the change updates the tool everywhere it appears.

The audience selector also appears alongside things you have already shared, so it is clear who can see each post. After you have shared a post, you have the option to change who it is shared with. If you want to change the audience of a post after you have shared it, click the audience selector and select a new audience. Remember, when you post to another person's Timeline, that person controls what audience can view the post. Additionally, anyone who gets tagged in a post may see it, along with their friends.

How do I control who can see what's on my profile and Timeline?

Here is an overview of who can see what is on your profile and tools you can use to control what you share on your profile and Timeline.

Overview

- You can share basic information like your hometown or birthday when you edit your profile. Click Update Info (under your cover photo) and then click the Edit button next to the box you want to edit. Use the audience selector next to each piece of information to choose who can see that info.
- Anyone can see your public information, which includes your name, profile picture, cover photo, gender, username, user ID (account number), and networks (learn why).
- Only you and your friends can post to your Timeline. When you post something, you can control who sees it by using the audience selector. When other people post on your Timeline, you can control who sees it by choosing the audience of the Who can see what others post on your Timeline setting.

Tools

- As you edit your info, you can control who sees what by using the audience selector.
- Before photos, posts and app activities that you are tagged in appear on your Timeline, you can approve or dismiss them by turning on Timeline review. Keep in mind, you can still be tagged, and the tagged content (ex: photo, post) is shared with the audience the person who posted it selected other places on Facebook (ex: News Feed and search).
- Set an audience for who can see posts you have been tagged in on your Timeline.
- To see what your profile looks like to other people, use the View As tool.


Where are my privacy settings?

Your privacy settings page has a group of general controls for your Facebook account.

To view and adjust your privacy settings:

1. Click ▼ in the upper-right corner of any Facebook page
2. Select Settings from the dropdown menu
3. Select Privacy on the left
4. Click a setting (ex: Who can see your future posts?) to edit it

You can also quickly view and adjust some of the most used privacy settings and tools from your

 Privacy Shortcuts at the top right of any Facebook page.

To control the privacy for posts, photos and other stuff you share on your Timeline, you can choose your audience when you post.

Who can add me as a friend?

By default, anyone on Facebook can add you as a friend. If you want to change who can send you friend requests:

1. Click ▼ in the top right of any Facebook page and select **Settings**
2. Click **Privacy** in the left column
3. Click **Edit** next to **Who can send you friend requests?**
4. Select an audience from the dropdown menu

How do I remove a tag from a photo or post I'm tagged in?

Hover over the story, click  and select Report/Remove Tag from the dropdown menu. You can then choose to remove the tag or ask the person who posted it to take it down.

You can also remove tags from multiple photos at once:

1. Go to your activity log
2. Click **Photos** in the left column
3. Select the photos you'd like to remove a tag from
4. Click **Report/Remove Tags** at the top of the page
5. Click **Untag Photos** to confirm

Removed tags will no longer appear on the post or photo, but the post or photo is still visible to the audience it's shared with. People may be able to view the post or photo in places like News Feed or search results. To fully remove it from Facebook, ask the person who posted it to take it down.

Last edited about 2 months ago


Permalink • Share • Related articles

Was this answer helpful?

What is Timeline review? How do I turn Timeline review on?

Timeline review lets you choose whether posts you're tagged in appear on your Timeline. Keep in mind that posts you are tagged in can also appear in News Feed, search and other places on Facebook.

When people you are not friends with tag you in a post, they automatically go to Timeline review. If you want to review tags by friends, you can turn on Timeline review for tags from anyone. To turn on Timeline review:

1. Click  at the top right of any Facebook page and select Settings
2. In the left column, click Timeline and Tagging
3. Look for the setting **Review posts friends tag you in before they appear on your Timeline?** and click **Edit** to the far right
4. Select Enabled from the dropdown menu

Last edited about 11 months ago

Permalink • Share • Related articles

Was this answer helpful?

How do I review tags that people add to my posts before they appear?

Tag review is an option that lets you approve or dismiss tags that people add to your posts. When you turn it on, any time someone tags something you posted, that tag will not appear until you approve it.

To turn on tag review:

1. Click ▼ at the top right of any Facebook page and select Settings
2. In the left column, click Timeline and Tagging
3. Look for the setting Review tags people add to your own posts before the tags appear on Facebook? and click Edit to the far right
4. Select Enabled from the dropdown menu

When tag review is enabled, you will get a notification when you have a post to review. You can approve or ignore the tag request by going to the post.

Note: When you approve a tag, the person tagged and their friends may see your post. If you don't want your post to be visible to the friends of the person tagged, you can adjust this setting.

How do I control who sees posts and photos that I am tagged in on my Timeline?

To choose who can see posts you've been tagged in after they appear on your Timeline:

1. Click ▼ at the top right of any Facebook page and select **Settings**
2. In the left-hand column, click **Timeline and Tagging**
3. Look for the setting **Who can see posts you have been tagged in on your Timeline?** and click **Edit** to the far right.
4. Choose an audience from the dropdown menu

Twitter

The default setting for Twitter is to allow anyone to follow you and you to be able to follow anyone whose account isn't protected. They can read your tweets plus any tweet with your name in it, you can read theirs plus any tweet with their name in it. Your profile is open to public view, along with your list of followers and those you follow.

To let only people you approve follow your tweets, "**Protect**" your tweets through Settings and then the Account tab. Check "Protect my tweets" and click the "Save" button. You will then receive e-mails letting you know that someone wants to follow you, and you can okay them after looking at their profiles.

If you protect your account later, it won't protect you from people who followed you before you protected it. So, go back through your followers and weed out unsavoury characters you now don't want to follow or who have followed you.

If you don't automatically protect your tweets, consider periodically gleaning your followers and those you follow to clean out spammers and other unsavoury accounts.

If someone unsavoury follows you or interacts with you unfavourably, you can block them. Click on their name (that will take you to their profile page) and look for the "block" link on their page.

YouTube

The default setting for YouTube is that the videos that you post are viewable for the public, anyone can post a comment about your videos, anyone can see your profile, and anyone can message you. You can change those settings if you choose, and you can block users.

To make changes to the default settings, sign in to your YouTube account and under your name at the top of the page, select "Account". That will take you to the "Overview" page.

Under Profile, you can decide how much personal information to divulge.

Under Privacy, you can change search and contact restrictions and make advertising settings.

Under Sharing, you can change activity feeds and auto share options.

Under Customize Homepage, you can change what modules you want to see on your YouTube page.

While in Overview, under More > Edit Channel you can decide whether to allow others to find your channel (your account) if they have your e-mail address.

If someone is making comments about your videos that you find distasteful, block their comments by clicking the "Block User" button in the "Connect with" box in their profile. You can block everyone from commenting, too.

To make a video that you've uploaded private, go to Account > Uploaded Videos and choose the video(s) you want to make private. Under the "Broadcasting and Sharing Options" section, find the "Privacy" options and click the little black arrow to see the option to make the video public or private.

To make a Playlist private, go to Account > Playlists under "My Videos." Select the Playlist you want to make private.

You can create a Group to focus your YouTube communications on your organization go to Account > Groups, then click "Create a Group". After you've filled in all the information, click the "Create a Group" button. You will then be directed to a blank Group homepage where you'll invite Group members, post videos for the Group, and so on.

Mobile phone security

Mobile phones are an integral part of our daily communications. All mobile phones have the capacity for voice and simple text messaging services. Their small size, relatively low cost and many uses make these devices popular. In Zimbabwe the mobile penetration rate is more than 100 percent.

Recently, mobile devices with many more functions have become available. They may feature GPS, multimedia capacity (photo, video and audio recording and sometimes transmitting), data processing and access to the internet. However, the way the mobile networks operate, and their infrastructure, are fundamentally different from how the internet works. This creates additional security challenges, and risks for users' privacy and the integrity of their information and communications.

It is important to start with the understanding that mobile phones are inherently insecure:

- **Information sent from a mobile phone is vulnerable.**
- **Information stored on mobile phones is vulnerable.**
- **Phones are designed to give out information about their location.**

People often carry mobile phones that contain sensitive information. Communications history, text and voice messages, address books, calendar, photos and many other useful phone functions can become highly compromising if the phone or the data is lost or stolen. It is vital to be aware of the information that is stored, both actively and passively, on your mobile phone. Information stored on a phone could implicate the person using the phone as well as everyone in their address book, message inbox, photo album, etc.

Mobile phones that connect to the internet are also subject to the risks and vulnerabilities associated with the internet and computers, as discussed in our other tactics guides regarding information security, anonymity, information retrieval, loss, theft and interception.

In order to reduce some of these security risks, users should be aware of their phone's potential for insecurity, as well as its set-up options. Once you know what the possible problems may be, you can put safeguards into place and take preventative measures.

Physical security for your mobile phone

As is the case with other devices, the first line of defence for the safety of the information on your mobile phone is to physically protect the phone and its SIM card from being taken or tampered with.

- Keep your phone with you at all times. Never leave it unattended. Avoid displaying your phone in public.
- Always use your phone's security lock codes or Personal Identification Numbers (PINs) and keep them secret [unknown to others]. Always change these from the default factory settings.
- Physically mark (draw on) the SIM card, additional memory card, battery and phone with something unique and not immediately noticeable to a stranger (make a small mark, drawing, letters or numbers, or try using ultra-violet marker, which will be invisible in normal light). Place printed tamper-proof security

labels or tape over the joints of the phone. This will help you easily to identify whether any of these items have been tampered with or replaced (e.g. the label or tape will be mis-aligned, or leave a noticeable residue).

- Make sure that you are aware of the information that is stored on your SIM card, on additional memory cards and in your phone's memory. Don't store sensitive information on the phone. If you need to store such information, consider putting it on external memory cards that can easily be discarded when necessary – don't put such details into the phone's internal memory.
- Protect your SIM card and additional memory card (if your phone has one), as they may contain sensitive information such as contact details and SMS messages. For example, make sure that you do not leave them at the repair shop when your phone is being serviced.
- When disposing of your phone make sure you are not giving away any information that is stored on it or on the SIM or memory card (even if the phone or cards are broken or expired). Disposing of SIM cards by physically destroying them may be the best option. If you plan to give away, sell or re-use your phone make sure that all information is deleted.
- Consider using only trusted phone dealers and repair shops. This reduces the vulnerability of your information when getting second-hand phones or having your phone repaired. Consider buying your phone from an authorised but randomly chosen phone dealer – this way you reduce the chance that your phone will be specially prepared for you with spying software preinstalled on it.
- Back up your phone information regularly to a computer. Store the backup safely and securely. This will allow you to restore the data if you lose your phone. Having a backup will also help you remember what information might be compromised (when your phone is lost or stolen), so you can take appropriate actions.
- The 15-digit serial or IMEI (International Mobile Equipment Identity) number helps to identify your phone and can be accessed by keying *#06# into most phones, by looking behind the battery of your phone or by checking in the phone's settings. Make a note of this number and keep it separate from your phone, as this number could help to trace and prove ownership quickly if it is stolen.
- Consider the advantages and disadvantages of registering your phone with the service provider. If you report your phone stolen, the service provider should then be able to stop further use of your phone. However, registering it means your phone usage is tied to your identity.

Basic functions, trackability and anonymity

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

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

- Make calls from different locations each time, and choose locations that are not associated with you.
- Keep your phone turned off, with the battery disconnected, go to the chosen location, switch your phone on, communicate, switch the phone off and disconnect the battery. Doing this habitually, each time you have to make a call, will mean that the network cannot track your movements.
- Change phones and SIM cards often. Rotate them between friends or the second-hand market.
- Use unregistered pre-paid SIM cards if this is possible in your area. Avoid paying for a phone or SIM cards using a credit card, which will also create a connection between these items and you.

About eavesdropping

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

look as though they are switched off.

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

About interception of calls

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

Conversations between Skype and mobile phones are not encrypted either, since at some point, the signal will move to the mobile network, where encryption is NOT in place.

Security settings for android smartphone

1.1 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, without 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.

1.2 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.

1.3 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.

1.4 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 to 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.

1.5 CALLER IDENTITY

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

1.6 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:

1. The phone operating system: go to: *settings* -> *About phone* -> *updates* -> *check for updates*.
2. 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.

2. APPS FOR ANDROID

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: allows you to 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 recognise 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.

RedPhone

License: FOSS [GPL v3] / **Requirements:** Android 2.3 and up.

Details: Allows you to make encrypted phone calls over the internet. A valid phone number is required to register.

TextSecure

License: Freeware [GPL v3] / **Requirements:** Android 2.3 and up.

Details: is an app to send encrypted text messages [SMS] via your phone provider and encrypted messages over WiFi and your phone internet connection as well as storing all SMS and messages in an encrypted container on your phone.

2.2 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: Antivirus 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: 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.

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: Allows 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: 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.



Backup - An extra copy of computer files, usually kept physically separate from the originals. Essential for recovery when original files are damaged or lost.

Digital signature - A way of using encryption to prove that a particular file or message was truly sent by the person claiming to have sent it. A digital signature typically depends upon three elements: public key encryption, a Certificate Authority and a digital certificate.

End-to-end encryption - The way data is protected by encoding it at the starting point and then decoding it at the destination. The sender and the receiver are the only ones with the encryption key so noone can eavesdrop. Examples of end-to-end encryption include PGP for email and OTR for instant messaging.

HTTPS - A variation of the web communication standard HTTP [HyperText Transfer Protocol] enabling secure data transmission. You can usually see if you are using HTTPS in the upper left corner of your browser's address bar.

IP address (Internet Protocol address) - A unique identifier assigned to your computer when it is connected to the Internet. Masking your IP address can help disguise your location and other personal details.

Linux - An open source version of the UNIX operating system considered to be very secure.

Keylogger - Software that monitors and captures everything a user types into a computer keyboard. Used for technical support and surveillance purposes. Can also be integrated into malware and used to gather passwords, user names, and other private information.

Malware - Derived from "malicious software." Software designed to do harm by causing damage to systems or data, invading privacy, stealing information, or infiltrating computers without permission. Includes viruses, worms, Trojan horses, some keyloggers, spyware, adware, and bots.

Virus - A programme that can self-replicate and infect files, programmes, and computer systems. Some viruses simply replicate and spread themselves, while others can also damage your computer system and data.

Open source software - Computer software with a source code that can be seen, modified and distributed freely. Open source software is generally considered a safer alternative than proprietary software because developers can test or audit it to detect any backdoors.

OTR (Off The Record) - Cryptographic protocol used for encrypting instant messaging conversations. For example, OTR is used with the Pidgin instant messaging program.

PGP (Pretty Good Privacy) - A freeware program primarily for secure electronic mail. Alternative: GnuPG. OpenPGP is a protocol for encrypting email using public key cryptography and is based on PGP.

Adware - Software that displays advertising content on your computer. Like its cousin spyware, some adware runs with your full knowledge and consent, some does not. More often an annoyance than a security risk, adware may also monitor browsing activities and relay that information to someone else over the Internet.

Spyware - Software that collects information about your computer and how you use it and then relays that information to someone else over the Internet. Spyware ordinarily runs in the background and often installs itself on your computer without your knowledge or permission.

SSL (Secure Sockets Layer) – a standard security technology that allows sensitive information such as credit card numbers, social security numbers and login credentials to be transmitted securely.



TLS (Transport Layer Security) – A protocol for encrypting web, email and other stream-oriented information sent over the Internet. It is derived from the SSL protocol.

Tor (The Onion Router) – An anonymity tool that allows you to bypass Internet censorship and hide the websites and Internet services you visit, while also disguising your own location.

Virus – a programme or code that replicates itself onto other files with which it comes into contact. Most viruses only replicate, although many can do damage to a computer system or a user's data as well.

VPN (Virtual Private Network) – A secure network that comes in handy when you surf on open Wifi networks in cafés, libraries, etc. since it encrypts your Internet traffic, keeping it from prying eyes.



www.misazim.com  [@misazimbabwe](https://twitter.com/misazimbabwe)  [MISA Zimbabwe](https://www.facebook.com/MISA.Zimbabwe)

84 McChlery Avenue, Eastlea, Harare, Zimbabwe