

Election Reporting and Safety Guidelines



**AMBASSADE
DE FRANCE
AU ZIMBABWÉ**

*Liberté
Égalité
Fraternité*

Published By:

Media Institute of Southern Africa
Zimbabwe Chapter (MISA Zimbabwe)
+263242776165, +263242746838
Website: zimbabwe.misa.org

Supported by the French Embassy in Zimbabwe

<https://zw.ambafrance.org/-Ambassade-de-France-a-Harare->

Design & Layout

OnaDsgn
hello@onadsgn.com
www.onadsgn.com

ISBN: 9781779065353



This work is licensed under a Creative Commons
Attribution-NonCommercial 4.0 International License.

Contents

Introduction	04
Reporting Elections	06
The Journalist's toolbox	12
Safety and security	14
Broad guiding recommendations	19
First Aid Training & Mental Health Support	59
Creating the ideal environment	60
Fact-checking & Disinformation	63
Essential guidelines	66
ZEC and electoral processes	70

Reporting Elections and Safety Guidelines

Introduction

This handbook is dedicated to professional journalists working in the media in Zimbabwe, whose watchdog role and skills to fair, accurate and balanced reporting is severely tested during national elections.

Besides looking at the professional demands around reporting elections, this guide also focuses on the safety and security of journalists, mental health support and the need for fact-checking and information verification in a world struggling with “fake news”.

MISA Zimbabwe subscribes to the notion that ‘elections define democracy while the media enlightens and sustains it.’

For journalists, covering general elections is one of the most exciting experiences, but very demanding professionally.

While the stakes might be high for the candidates and the competing parties, and the welfare and future of countries and could be in court, the media will be under serious spotlight on how it covers the elections.

The media’s traditional role is to inform the public on issues of the day accurately and fairly, and to do so while respecting a professional code of ethics.

This obligation is more critical during elections where citizens vote in leaders for central or local government authorities. Voters look up to the media to inform them factually and fairly on the various parties, policies, personalities and programmes at play. This places a big responsibility on the media and on the journalists, underlining the fact that the election story “begins yesterday and not today” – it begins months before polling and can continue way after the votes have been tallied.

Although the election story could be regarded as a “set piece” easier to report, in practice covering elections requires more professional skills than the usual run-of-the-mill story.

MISA Zimbabwe recognises this fact, and through this handbook seeks to equip Zimbabwean journalists with guidelines on covering elections, some safety and security tips, managing mental health and rigorous fact-checking as the problem of misinformation and disinformation is acute during an election season.

In that regard, MISA Zimbabwe sincerely appreciates the financial assistance of the French Embassy in Harare in the production of this handbook.

Reporting Elections: “What can be difficult about the election story?”

What is difficult is the story has to be defined, and it must be defined very accurately.

What is difficult is that is to get the timelines right, to pick up the salient and important points and pegs, to project and package it interestingly.

The challenge is to remain professionally faithful to the needs of the public for accurate information in a field of political spin, propaganda and partisan presentation and posturing.

MISA Zimbabwe recognises that only in this way can the media play its fundamental role in the process of democratisation, good governance, transparency, accountability and respect for human dignity.

While the media should at all times conduct itself professionally and within the confines of the profession, this role becomes even more imperative during election time when the expectations for renewal or continuity of leadership to spur socio-economic development, peace and stability takes centre stage.

Since 2000, Zimbabwe’s parliamentary, presidential and local government elections have been variously described as “historic,” a “landmark,” a “watershed,” “a-life-or-death-affair,” “a do-or- die-issue” and a “make-or-break” situation.

The elections have invariably taken place against the backdrop of social hardships, including an economic meltdown and a fierce contest that heightened fears of a political conflict. The challenge for the media and journalists has been to contextualise, interpret and articulate the citizens' concerns and expectations.

The media has a responsibility to provide the public with access to different facts, opinions and ideas within the framework of the expectations of the citizens and to hold authorities, appropriate officials accountable, to promote the rule of law and respect for human rights.

The media has a duty to inform voters on the election manifestos and campaigns of political parties and candidates while also focusing on the socio-economic and political issues, and helping the public to understand the electoral processes.

But the media must do all this while upholding its professional ethics to cover stories without seeking bribes, paying for information, using illegal means to source information, betraying confidences, exposing the innocent to physical or political danger.

On their part, journalists must cover stories and operate in a possibly hostile environment with the greatest care for their own welfare and lives.

The Cardinal Trio

Journalists covering elections need to develop a sharp sense of professionalism with a clear focus on expanding:

1. knowledge of the issues of the day, context and background
2. technical or reporting skills to present stories factually, accurately, fairly and with judicious balance
3. commitment to ethics and high moral standards

The cardinal trio is a concept that addresses issues of responsibility, processes, preparation, projection, presentation, knowledge and skills. It is about responsibility to pick and read important issues at the right time, to highlight and interpret the issues and processes, to prepare and present the stories in an interesting way and to acquire knowledge and skills appropriately.

The first major requirement is to understand the political environment. What are the rules of the game? What does the law say about the various processes, and who is responsible for the different aspects of these laws and regulations?

What is the practical meaning or impact of these statutory provisions? How different is it from the practice elsewhere in the region, in Africa, around the world?

In their 2009 book: *Eyes of Democracy, The Media and Elections*, Kenyan journalists Manoah Esipisu and Isaac Khaguli, firmly frame the point that part of the media's

role is to “enlighten and sustain” democracy.”

But they caution that it is not an easy job:

“Covering elections presents a big challenge to the media, especially in developing countries where the average age in the newsroom has dropped significantly. Tight deadlines, knowledge of relevant legislation, the political players and process, adherence to the basic ethics and increasingly questions of personal safety all pile pressure on the media.”

In the case of Zimbabwe, journalists must familiarise with laws and regulations governing or likely to have an impact on their work such as the the electoral system, and:

- The Zimbabwe Electoral Acts and any proposed legislation
- Zimbabwe Electoral Commission Act (ZEC)
- Zimbabwe Media Commission (ZMC)
- Interception of Communications Act
- Maintenance of Public Order (MOPA)
- Citizen laws
- SADC Principles and Guidelines Governing Democratic Elections
- Miscellaneous Offences Act
- Freedom of Information Act
- Delimitation reports
- ZEC Regulations on the conduct of the media, political parties, etc
- Criminal Law (Codification and Reform) Act
- Cyber and Data Protection Act

This seems to be a lot to master, and it probably is. But journalists must have the humility to accept the need for education and awareness.

An ignorant journalist who has a limited grasp of issues/ subjects/processes is not only susceptible to manipulation by scheming spin doctors, but also risks losing credibility and respect in the eyes of discerning readers.

The media must be accountable for journalism that is committed to accuracy, balance and fairness. Whatever the circumstances, citizens in any democracy are united by three rights:

- The right of voters to make a fully informed choice.
- The right of candidates to put their views across.
- The right of the media to report and express its views on matters of public interest.
- Other good practices for the media include:
- Regulatory authorities ensuring that media coverage of elections meets legal requirements.
- That media houses have a code of conduct to guide its coverage of elections accurately and fairly.
- That the media has access to public information on parties and personalities contesting elections.
- That the security of journalists and the media is secured during elections.

This brings us to the issue of journalists during elections:

- The lack of professionalism
- The loss of mental balance
- The use of intemperate language

- The inability to manage hate language
- The fear of physical attacks
- The exposure to bribes and begging
- The framing of partisan views
- The danger of ignorance
- The fatality of lack of creativity
- Lack training on issues of safety
- Lack of guarantee of media freedom
- Responsibility in reporting inflammatory speeches
- Poor crowd estimation skills
- Shrill propaganda
- The journalist's tool box

In Reporting Elections in Southern Africa, a media handbook published in 2000, pages 46-50.

- News reporting and current affairs programming should be primarily to inform the public of issues.
- Coverage of the party leaders and personalities should not be done at the expense of the main issues.
- Coverage of minor parties should not be disproportionate to their role in the election.
- Comment and editorial support should be clearly defined and not disguised as news.

A summary of the recommended election coverage model would include:

- Constitution
 - Economic indicators
 - Demographic profiles
 - Cultural and traditional practices
 - The parties and the issues
-

- The personalities and the programmes

Covering elections - a toolbox checklist:

1. A skills and knowledge audit.
2. A comprehensive plan, including a pre-campaign, a campaign, voting and post-balloting coverage plan.
3. A vote and political mapping exercise.
4. A refresher course on reporting elections (based on the skills and knowledge audit exercise).
5. Safety and Security guidelines.
6. Journalism professional code of conduct (ethics).
7. Fact sheets on the contesting parties and leading personalities.
8. Political maps (country, province, district, constituency, ward).
9. Delimitation reports and demographic profiles.
10. A bio/factsheet on voting systems (PR/ FPTP).
11. Package of laws/legislation governing the elections.
12. Manifestos, constitutions, code of conduct, and factsheets on major policies, programmes and plans.
13. Lists of candidates, short biographies and photos of key managers.
14. Comprehensive contact list of key personnel/spokespersons.
15. Statistics about resources, staffing, membership, budgets.
16. Major policy statements and or planned organisational reforms.
17. History of major programmes.
18. Position papers on major issues and external relations.

19. List of media houses, contacts, journalists, columnists, talk show hosts, and producers who report news and features in your field/organisation. (This information could include background on individual positions on programmes).
20. Comprehensive list of government agencies, legislators, and other officials with regulatory powers in different sectors.
21. Copies of relevant legislation, regulations, pending bills, referenda, government publications, parliamentary committee hearing reports and research work.
22. Diary of major events, anniversaries, conferences, including schedule of related national and international events.
23. Clippings from newspapers, magazines, and other media on major issues and problems around a party, a candidate or other related issue.
24. Major reports, transcripts and video recordings of radio and TV coverage.
25. Important reference books and results of results of credible surveys on major problems, programmes or projected polls.

Why secure

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

The benefits of technology are obvious – but there are security implications too. Potentially the more we use technology, there are a number of security risks for organisations as well as personal information. From bank accounts to personal photos and messages, we all have more than ever stored on digital devices and online accounts—and more to lose. All our private conversations are out there somewhere. But for those who weren't born with an iPad, 'digital security' might as well be a foreign language.

The cyber security context for human rights defenders in Zimbabwe is characterised by a range of risks and threats. The government has long been accused of using its intelligence and security apparatus to monitor and target civil society activists, journalists, and human rights defenders.

This includes the use of surveillance technologies, including through the use of spyware, to monitor their activities.

In addition, the government has imposed various restrictions on freedom of expression, including through

the criminalisation of online activities. For example, the government has used the country's new cybercrime laws to target and prosecute individuals who criticise the government online.

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

1. Information or Data Loss.

- a. When your hard drive dies, your computer is affected by a power surge, your phone gets
- b. smashed, or you lose your camera's data card, or even water or fire damage
- c. When affected by malware (malicious software). Some viruses can destroy data on your computer or mobile device
- d. When you forget your password

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

- a. When your computer mobile device, flash disk, or SIM card is lost
- b. When someone gets hold of your password to your computer service like email, cloud storage (like drop box, google drive)

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

- a. When network services are blocked or stop working
- b. 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
- c. When affected by malware (malicious software). Some viruses can destroy data on your computer or mobile device
- d. When you forget your password

Physical security related risks:

We do a lot of digital work to protect sensitive information. But that is only one aspect of digital security. The work you do to protect your valuable devices and documents can be undone in an instant if your devices are lost, stolen, tampered with, confiscated, or damaged. Planning for physical security is as important as protecting your devices digitally.

As we see in the news on a daily basis, the chances of your phone or laptop being stolen are uncomfortably high. So, what would happen if your mobile device falls into the wrong hands? Before we get into the various tips and tricks for securing your computer or mobile device, remember that keeping your device safe is the first step towards digital security.



Devastated: NewsDay senior staff (from left) Assistant Editor Tangai Chipangura, Political Editor Kelvin Jakachira, NewsDay Editor Brian Mangwende, Chief Sub Editor Kamurai Mudzingwa and Senior Assistant Editor Wisdom Mdzungairi view the ransacked computers.

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

Here is what happened to the Newsday, The Daily newspaper, NewsDay, has reported that its offices were broken into Monday evening. A laptop belonging to its editor and several hard drives from computers used by

journalists were stolen. On Monday evening ‘unknown criminals,’ as the paper put it, broke into the offices and stole ‘vital information and data’ contained in the hard drives, including a laptop belonging to the editor Brian Mangwende. Coincidentally the ‘thieves’ also targeted a computer belonging to Langa, the victim of the army inquiry last week.

Source : <http://www.zimeye.com/sensitive-data-stolen-in-raid-on-newsday-offices/>

**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”) is any programme or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojan horses, and also spyware, a 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 colorfully-named categories. Worms, macroviruses, trojans and backdoors are some of the more well-known examples. Many of these viruses spread over the Internet, using email, malicious webpages 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 they contract viruses.

So many of the suggestions above are also helpful when defending against this second class of malware. Because malicious webpages 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.

Online security

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

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 optimise 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. 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, earlier this year, it was discovered that some Chrome extensions can change service or ownership without notification to users. As a result, Chrome's regulations for extensions are changing this June 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, and 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

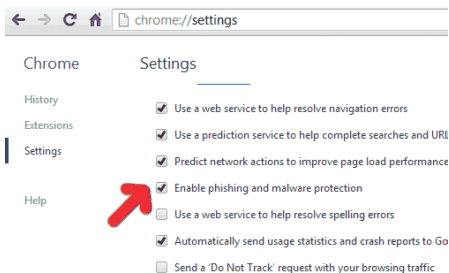
crowd-sourced from WOT's global user base and are supported by trusted third-party sources, such as up-to-date directories of malware sites.

- **LongURL.org.** If you're 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're 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:

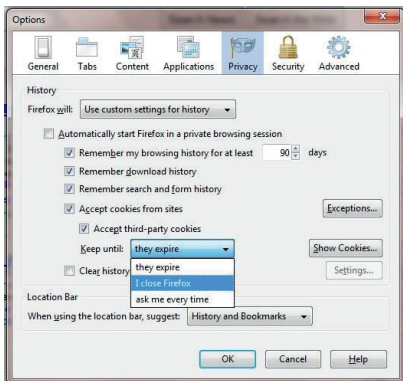
- Cookies: Select "Keep local data only until I quit my browser" and "Block third-party cookies and site data." These options ensure that your cookies will be deleted upon quitting Chrome and that advertisers will not be able to track you using third-party cookies.
- JavaScript: Select "Do not allow 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 Autofill and deselect “Offer to save passwords you 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.

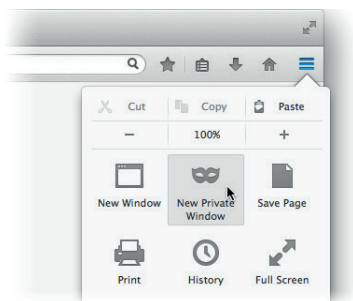
Now, while private browsing is useful, it’s not all powerful. Private browsing won’t protect you from keyloggers, tracking programmes, nasty viruses after your personal info, or government surveillance efforts. But as far as the average Joe is concerned, your private online activities will remain shrouded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

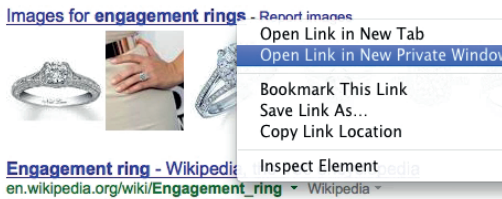
Click the menu button  and then click New Private Window.



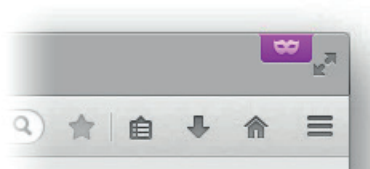
Open a link in a new Private Window

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

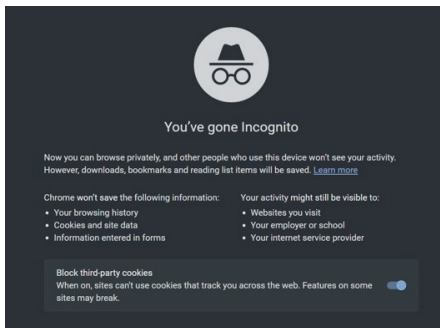
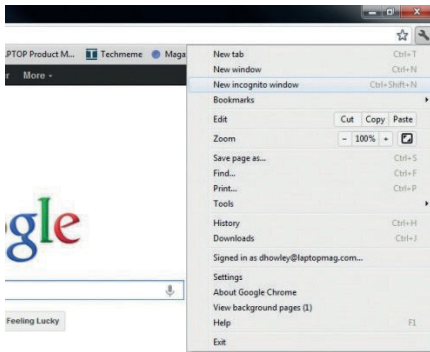
Tip: Private Browsing windows have a purple mask at the top.



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

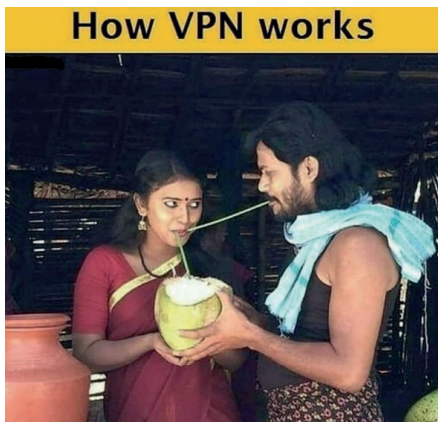


1. Open a Chrome window
 2. In the top-right corner of the browser window, click the Chrome menu. ≡
 3. Select New Incognito Window.
 4. A window will open with a gray figure in the top-right corner 🧑
 5. To close incognito mode, go to the corner of each of your incognito windows and click the X.
- Tip:** You can also press Ctrl + Shift + N (Windows, Linux, and Chrome OS) and ⌘ - Shift - N (Mac) to open an incognito window.



Psiphon

Psiphon is a circumvention tool for Mobile phones and Windows. Used as an engine for internet freedom, this VPN (Virtual Private Network) application is user-friendly and protects the users from censorship by providing unlimited access to the internet. Psiphon helps internet users bypass content-filtering systems used by governments in countries like Zimbabwe.



Why use Psiphon?

VPN's have become increasingly popular and reliable in this internet age where some government authorities

are suppressing access to information by regulating the internet. Zimbabwe has experienced the shutdown of social media services, with Internet Service Providers (ISPs) Econet Wireless, NetOne Zimbabwe, Telecel Zimbabwe, Liquid Home and Tel One Zimbabwe being ordered to block access to subscribers. Psiphon gives the user unlimited access to the internet by providing encrypted tunneling that secures 100% of all your internet access and routing for all applications. In simpler terms, if you want to protect your browsing from prying eyes or when the government blocks some internet services, **Psiphon** provides much needed circumvention and protection,

Which devices can use **Psiphon**?

Android and iOS mobile phones as well as Windows (tablets, laptops).

How to install **Psiphon** on Android/iOS

1. Go to Google Playstore/iOS app store
2. On the search engine tab, type in 'Psiphon'.
3. Tap on the latest Psiphon application and download.

Application is free.



4. Wait for the app to install onto your Android or iOS supported device
5. After installing, you will be taken through the standard terms and conditions

6. You will be taken to the app's homepage, which will give you access to the Psiphon browser where you can surf and download with no limit on how much data you can consume, user stats (which show you how much data you are using).



7. Redirect your IP address by choosing your preferred region.
8. Start browsing! Remember, the app is completely safe and Psiphon makes sure your connection is secure from any tracking.
9. When you are through, press the stop button (at the bottom left corner for mobile users) and you are disconnected from the VPN.



How to install Psiphon for Windows 11, 10, 8, 7 PC

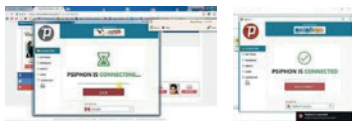
1. Go to Google Play Store or straight to the Psiphon website and download the installation file of the



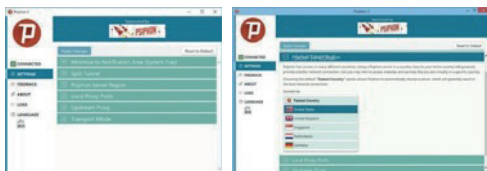
- software. Save it on your computer
2. After downloading the file, open it by letting it run on

your PC. You will be taken through the normal terms and conditions.

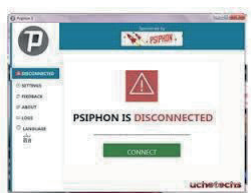
3. You will be redirected to the Psiphon home page.



4. Before browsing, configure settings to your satisfaction by clicking on the settings tab.
5. Select your preferred server region, to keep away the prying eyes!



6. Browse and download with no fear of tracking or restrictions!
7. When you are through, press the disconnect button and you will exit the app.



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 near 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:

1. Information sent from a mobile phone is vulnerable.
2. Information stored on mobile phones is vulnerable.
3. 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 defense 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 pass code option. 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 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 hand phones or having your phone repaired. Consider buying your phone from an authorised 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.

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.

1. Never let people whom you don't trust get physical access to your phone; this is a common way of installing spying software on your phone.
2. 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.
3. Make sure that any person with whom you communicate also employs the safeguards described here.
4. 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.

1.SECURITY-RELATED SETTINGS FOR ANDROID

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

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

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

Note: When updating your phone's 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 free WIFI hotspot.

1.CHECK YOUR APP PERMISSIONS

Review all permissions one by one to make sure only apps you use can use them. The following permissions should be turned off in apps you do not use, and considered suspicious when used by apps you do not recognise:

- Location
- Contacts
- SMS
- Microphone

- Voice or speech recognition
- (Web)camera
- Screen recording
- Call logs or call history
- Phone
- Calendar
- Email
- Pictures
- Movies or videos, and their libraries
- Fingerprint reader
- Near field communications (NFC)
- Bluetooth
- Any setting with “disk access,” “files,” “folders,” or “system” in it
- Any setting with “install” in it
- Facial recognition
- Allowed to download other apps

2. TURN OFF LOCATION AND WIPE HISTORY

Get in the habit of turning off location services overall, or when you are not using them, for your whole device as well as for individual apps.

Regularly check and clear your location history if you have it turned on. Location settings may be in slightly different places on different Android devices, but are probably somewhere in Settings, Privacy, and/or Security as well as your Google account preferences.

3. SET YOUR SCREEN TO SLEEP AND LOCK

Set your screen to lock a short time after you stop using it (try setting it to 1 minute or 5 minutes and see which

works for you.

Use a long passphrase (minimum 10 characters), not a short password or PIN. Making it possible to use your fingerprint, face, eyes, or voice to unlock can be used against you by force; do not use these options unless you have a disability which makes typing impossible. Remove your fingerprints and face from your device if you have already entered them. Android devices differ, so this could be in a few locations on your device, but try looking where you would normally find your device lock settings. Pattern locks can be guessed; do not use this option. Simple “swipe to unlock” options are not secure locks; do not use this option. Disable “make password visible” option.

Set a long password.

Set your device to sleep after a short period of time and require a password to unlock on waking. The place to do this will be different on different devices, but it may be under “Display,” “System,” or “Security.”

Social Media security

Social media has become an integral part of people’s lives as it is a primary channel through which we access information and interact with others. The COVID-19 pandemic has only exasperated this, as isolation pushed people to lean even more on social media platforms as their primary connection to the rest of the world. This has resulted in an increase in the amount of information people are sharing.

1. Think before you share

What is posted on social media is not necessarily only seen by the friends and family with whom you are directly connected. Depending on your account settings, what you post could be seen by anyone and everyone. And this isn't limited to what you post, but also what posts or photos you are tagged in, groups you are part of or interests you follow.

Cybercriminals frequently leverage publicly accessible social media information to tailor their attacks. The process, which is one aspect of Open Source Intelligence (OSINT), allows them to target specific individuals for an attack, or profile broad groups of people to attack.

You may be thinking, "I'm not interesting, so that wouldn't happen to me." But that is not a safe way to think about social media security.

Any employee can be targeted as a point of entry for a corporate level attack. Your profile tells a lot about you and might inspire a targeted phishing email or vishing call or text that results in an organisation network compromise.

1.1 Common social media sharing mishaps include:

Workplace photos that expose details about your employer: First day of work photos with an ID badge can allow an attacker to create their own badge to walk through your workplace without question.

Passwords or account details can be seen on sticky notes

or visible on screens in a photo. Even the type of laptop, email client, browser or phone system you use could fuel an informed and convincing phishing attack.

Personal posts can result in professional attacks: a new car photo in front of your house can reveal your address and other information. Credit cards, driver's licenses, passports, and any other personal identifiers can be found in the background (or forefront) of images on social media.

All of this personally identifiable information (PII), can put your identity at risk, and it can be used to impersonate you to your employer for a corporate attack.

Any photo with geolocation enabled can let criminals know you're out of town and your home is empty. And photos can be easily reverse searched to find out additional information.

Having a phone number and email address associated with your social media accounts may be required for the account or requested for security purposes, but check the settings to make sure they don't make you or the account vulnerable.

1.2 Practice good account hygiene

Because software that cracks passwords is always getting better, what we used to think was a strong password may no longer be enough to keep us safe.

Passphrases are much stronger than passwords – the more

complex and unusual, the harder it will be to crack. These involve a sentence that contains a mix of letters, numbers, and special characters. If you are wondering how in the world, you will remember all these different passphrases, consider using a secure password manager.

It is also important to be careful about which email accounts you are linking to your social media.

Organisations should put in place a policy that prohibits the use of corporate emails with social media accounts. This will make it harder for attackers to use stolen social media account credentials to get into corporate networks. It's best to use a separate email address for each social media account. If your account gets hacked, an attacker won't have access to as much valuable information.

1.3 Some additional best practices to follow are:

Use a different password for every account. This way if one account is compromised, other accounts may not suffer the same fate.

Enable multifactor authentication (MFA) for an additional level of security.

Keep your apps updated. Just like any software, it is important to keep them up to date to ensure you are secure from any newfound threats or vulnerabilities. Delete any accounts that you no longer regularly use. This ensures they cannot be hacked and used to get into other accounts, like your email, that are linked to them.

1.4 Beware of fake news

Social media feeds are filled with a lot of fake news and misinformation. Fake news has existed for a long-time, and social media platforms are perfect for this type of nefarious activity. Sharing false information on social media is now even a service in the underground or “gray” market. It is important to remember this when browsing social feeds and to check the sources of links carefully before clicking or sharing.

To ensure you are not a victim, or a part of the problem by sharing fake news, you should be vigilant about what you click and share. Here are some ways to verify a post is real:

See if a news story has been reported directly on a reputable site or mainstream media: If it is real news, you can bet more than one media outlet is reporting on it. Look at the link: You can use similar principles that you use to protect yourself from phishing. Are letters in the URL replaced with similar characters?

Look at the quality: Are there real comments? Are there spelling and grammar mistakes? Is it a professional looking website?

Beware of clickbait headlines using hyperbolic terms. When browsing through social media feeds, you could use a mindset similar to the concept of Zero Trust. This means that you do not inherently trust anything, even if it is posted by a trusted person. Start from a place of Zero Trust and verify before deciding to trust a post. You never

know if your friend or another organisation may have been tricked and shared fake news, or their account may have been compromised.

Just because someone's bio says it is them, it doesn't mean it is. Don't trust someone by their bio alone.

You can keep the amount of information you share to a minimum by only giving permissions that are really needed and by actively managing your account settings.

Social media is a double-edged sword. It has been a lifeline during a very difficult time, allowing us to find another way to communicate, when the traditional, in-person method was unsafe. It allowed us to connect with loved ones and delivered critical information in a very uncertain time.

However, cybercriminals abuse it, and will continue to do so, as it is full of valuable data they can steal and is an easy platform for them carry out malicious plots. By using best practices, we can stay safe and reap the benefits that social media offers.

2. Facebook security

If you're relying more on Facebook to stay in touch, now's the perfect time to adjust your privacy and security settings. Here's how.

2.1. Clear your history using 'Off-Facebook Activity'

Facebook is constantly keeping tabs on your activity — on and off its site. Apps and websites automatically check if

you're still logged in and report what you're doing online back to Facebook.

This data used to be a well-kept part of Facebook's advertising strategy. Not anymore. Adjust and even delete what the company knows through a menu called "Off-Facebook Activity."

The Manage Future Activity tool acts as a more permanent version of Clear History. When you turn it off, it stops companies from sending Facebook ad-targeting data about you.

Keep in mind that disabling Future Activity prevents you from signing into other apps and websites with Facebook. To clear your history on the mobile app:

Tap the three-line menu in the bottom right of the Facebook app. Select Settings. Scroll down and select Off-Facebook Activity. Examine the apps that use your activity and make sure you want to remove the information. Tap Clear History.

To clear your history on the Facebook website: Click on the dropdown menu arrow at the top right of Facebook and click Settings & Privacy. Select Settings.

Tap Your Facebook Information in the left column. Click Off-Facebook Activity to review. From here, click Manage Your Off-Facebook Activity. You'll be asked to re-enter your password. Once you're verified, it will show

you the apps and sites that have shared ads with your Facebook account.

When you are ready to clear this information, click Clear History.

2.2 Hide your location

Facebook uses location data to serve you news or sell you things. If you disable location services, it won't use your precise location to target you with ads. Facebook still has access to your network location, so you'll need to turn off the feature on both your phone and the app.

To disable location services on an iPhone:

Go to the phone's Settings and tap Privacy. Tap Location Services, followed by Facebook. Tap Never to disable location services.

To disable location services on an Android phone:

Go to the phone's Settings and tap Privacy.

Tap Permissions Manager, followed by Location. Choose Facebook. Tap Deny to disable location services.

Once you're finished with adjusting your phone's permissions, follow these steps to disable location tracking in the app:

Tap the icon with the three lines in the bottom right.

Tap Settings & Privacy, followed by Privacy Shortcuts.

Tap Manage Your Location Settings, followed by Location Services. Tap Location and select Never.

2.3.Disable Facial Recognition

Facial recognition is central to Facebook's photo algorithm.

It's the reason you're automatically tagged in photos that others post.

You can disable facial recognition on the desktop version of Facebook. Follow these steps: Click the downward-pointing arrow in the top right of the screen.

Select Settings & Privacy, followed by Settings.

In the left column, click Face Recognition.

Tap "Do you want Facebook to be able to recognise you in photos and videos?" Select No in the drop-down menu to disable the setting.

3.4. Get rid of apps that track you off Facebook

When you use your Facebook username to log in to other platforms or websites, those companies can see your information and may be able to share your activity with Facebook.

This was one of the most significant issues behind the Cambridge Analytica scandal, leading to millions of people's profiles being harvested. Tap or click here for more details on Cambridge Analytica.

Thankfully, Facebook has changed its stance on third-party applications and lets users disable all that tracking.

Disable third-party app tracking from your desktop:

Click the downward-pointing arrow in the top right of the screen.

Select Settings & Privacy, followed by Settings.

Tap Apps and Websites on the left menu. Select Active.

Click on the box next to the app's name to stop tracking

you and click Remove. This will disable it from tracking you.

3.5. Enable two-factor authentication to lock out hackers

Two-factor authentication is one of the best ways to keep unwanted people from logging into your account. When someone tries to break into an account with 2FA enabled, they can't get in without a text-message code. Since the code goes to your phone, only you will be able to log in.

Activate 2FA from your desktop.

Click the downward-pointing arrow in the top right of the screen.

Tap Settings & Privacy, followed by Settings.

Select Security and Login.

Scroll down to Two-Factor Authentication and tap Use two-factor authentication.

Enter your phone number and confirm the code in the text to complete the setup.

Stop Google from showing your Facebook account:

Did you know your Facebook profile is indexed on Google? That means anyone looking up your name will be able to find your social media account, along with all the publicly visible data.

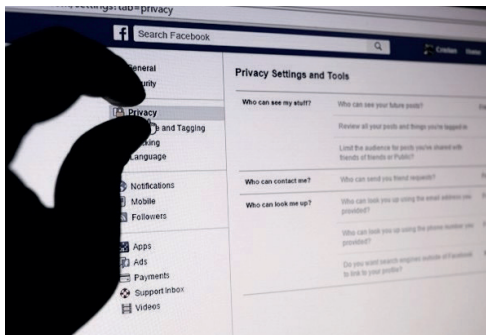
If you are not comfortable with this, we don't blame you. Google and people-search engines have a nasty way of making your private life public. Tap or click here to find out how to delete yourself from people-search sites.

With Facebook, at least, you can keep your profile out of searches. Follow these steps: On your computer, open Facebook and click the downward-pointing arrow in the top right of the screen.

Tap Settings & Privacy, then Settings followed by Privacy. Under “Do You Want Search Engines Outside of Facebook to Link to Your Profile?” click Edit. Click the checkbox on the bottom to turn off the setting.

Limit the audience for your personal posts

Not every friend on your list needs to know the intimate details of your life. This is even riskier when you factor in how many fake profiles are floating around. Tap or click to see how to spot the fakes. Limit the audience of your posts so only specific people can see them.



From your computer, follow these steps:

Open Settings & Privacy again, then Settings and click on Privacy.

Scroll down to Who can see your future posts? and click Edit. You can adjust the settings for specific audiences here.

Scroll down to Limit Past Posts to change who can access your previous content.

People accidentally share all kinds of personal facts and information without realising it.

Changing this setting can protect you from getting phished or stop a hacker from correctly guessing one of your security questions.

8. Stop your activity from being advertised (literally)

Ever seen an advertisement that tells you which of your friends Liked it? That is because Facebook automatically uses these endorsements to target ads to you and your friends. And if you Like something, your friends will see the same kinds of ads.

Of course, they're not asking your permission. But you can disable the setting to keep your interests and Likes more private. Follow these steps on your desktop:

Under Settings & Privacy, select Settings, then click Ads, followed by Ad Settings.

Click Social Interactions and select Only Me.

9. Avoid those Like and Share buttons on other parts of the web

Whenever you use a Facebook button on another website, you're feeding the beast that is Facebook's ad machine. Every Share, Like and recommendation, becomes part of the data feed that Facebook uses to tailor its algorithm.

Even if you have disabled tracking outside of Facebook, using these buttons is like permitting it to know what you are doing. You do not need to change any settings to avoid the pitfalls of these buttons. Just don't use them.

If you must share something, do it the old-fashioned way by copying and pasting it into a post.

10. Clean up your Friends List

Having a lot of Facebook friends means a larger audience witnessing your personal and private life. You probably don't need thousands of people to see the private ins and outs of your social life.

Plus, studies have shown that people who frequently accept new friend requests actually run a higher risk of being targeted by fake accounts.

For the sake of privacy, you are better off cleaning up your Friends list. To do this, open Facebook on your phone or computer and visit any one of your friends' profiles. Locate the button labeled Friends and click or tap it.

On the dropdown that appears, you will be able to select Unfriend. Do this for anyone you are not 100% sure about

or do not know closely. Facebook isn't a contest, and having more friends doesn't make your account more complete.

Safety of journalists

Another major primary concern during elections is that journalists covering elections must be able to work as safely as possible if they are to get their stories out. This means being able to survive, avoid injury and incarceration.

The most important thing is to remember that if the situation turns ugly do not be a hero. The assumption is that you will not be fired for refusing to do a job which puts your life at risk.

Precautions

- The news editor should always be briefed unstintingly on the dangers of a given assignment.
- The journalist's whereabouts should always be known to the news editor or a close family member for easy contact in case of an emergency.
- You should always have your cellphone at hand. In Zimbabwe it is advisable to possess two
- handsets of different networks because of the unreliability of the network services.
- Journalists should rally behind one another especially where it concerns the unlawful arrest, detention, assault and torture of colleagues.
- Never venture into hostile environments alone, you should always hunt in packs during election time.
- When venturing into volatile political areas,

- journalists should intuitively know when to retreat.
- Always re-evaluate the risks involved.
- Assigning editors should make the safety of their journalists paramount and discourage unwarranted risk-taking on the part of their journalists.
- Lower your profile during assignments in hostile territories and do everything possible not to attract attention to yourself for you will not only be a danger to yourself but to others.
- Get first aid training; it may help you or a colleague.
- Instinct, Intuition and Wisdom should be the operative words for those journalists working in hostile environments.

Other recommendations are:

- Never carry a gun or weapon
- Know the regulations which relate to an unrest area and where those areas are located.
- Be respectful of security personnel but you can challenge with confidence attempts to order you away from areas which you have legitimate right to be.
- Know where you are going and be adequately prepared before leaving; know what political, racial, religious or conflicts which exist: the information can help keep you out of trouble.
- Make contacts as soon as possible and get to know media representatives of all the major organisations in the area. Look for telephones and vantage points where you can cover an event without being too close if trouble seems possible.
- Be familiar with roads and where they lead to if you

have to leave suddenly.

- Learn and observe local community protocols and customs, including community leaders.
- Dress appropriately but inconspicuously, avoiding expensive jewellery and other items which may attract criminals. Learn the political colours of various parties and avoid wearing them.
- Be sure to have proper media accreditation which should be visible and define where you are
- legally allowed to visit around a polling station or electoral headquarters.
- If you are covering a potentially dangerous area, you have the right to ask your employer for insurance.
- Before leaving home, make sure you have arranged for contact with your office; telephone at pre-arranged times to file copy and to assure them of your safety and whereabouts. If your editor/producer does not hear from you, make sure they know how to contact you.
- When you are in the field listen to the locals. Pay attention to advice from people who live in a region/area.
- If you are caught in the middle of a disturbance, move away discreetly but do not run, you could become a target; avoid any confrontation.
- Respect the local dress code and err on the conservative side. Female journalists are encouraged to wear tights and have long-lasting sanitary pads.
- Be aware of how sources see you. You may be dressing appropriately, but still viewed as promiscuous because of culture misperceptions.
- Carry the cellphone number of someone senior in

the army or police. Threaten to report a would-be attacker to authorities.

- Always plot an escape route. Establish landmarks such as high trees or lampposts to get your bearings in case of a stampede.
- If a mob suddenly materialises, make sure someone is watching your back.
- Take a hotel room next to colleagues. (Unless they have been sexually harassing you, in which case stay on another floor.)
- Use doorknob alarms. They emit a loud noise if someone tries to break into the room.
- Keep a can of deodorant to spray into an attacker's eyes. It will temporarily blind, but won't cause lasting damage.

These tips have been culled from various sources. *

First Aid Training

Journalists need to get basic First Aid Training for handy skills in emergency situations where medical assistance may not be immediately available for your reporting team or colleagues.

It is advisable for those who have already received some training to do refresher courses.

Mental health support

While reporting elections is generally regarded as “exciting”, medical experts say the work carries a high risk of mental health problems for journalists operating in politically volatile or environments.

The risk is considered higher in media hostile situations

where and when journalists are associated with, or accused of partisan political reporting.

In such situations, media houses are encouraged to offer mental health support to journalists who may be suffering stress related problems, without even knowing it.

Technically mental health and psychosocial support (MHPSS) includes any support that people receive to protect or promote their mental health and psychosocial wellbeing. One major component of MHPSS is treatment and prevention of psychiatric disorders such as depression, anxiety and post-traumatic stress disorder (PTSD).

Creating the environment for effective coverage of elections:

Comprehensive Guidelines on Media Coverage of Elections in the SADC Region developed by MISA, the Electoral Commissions Forum of SADC countries (ECF-SADC), the African media project of the Friedrich-Ebert-Stiftung (FES), fesmedia Africa, and the Open Society Initiative for Southern Africa (OSISA), recommends that:

- Media houses provide adequate resources to their journalists for effective election coverage.
- The media enjoy unfettered editorial and programming independence from all vested interests including candidates, parties, media owners and organisations allied to and/or supporting candidates and political parties.
- All laws that hinder the media in fulfilling their role are repealed.
- All media are allowed access to all election activities including rallies, media conferences,

- candidates, parties and electoral management institutions and officials.
- Transparent polling procedures, fair, open counting of the votes and timely release of the results are guaranteed.
- Journalists and media houses can operate in an environment free of violence, harassment and intimidation.
- Sources and interviewees are not threatened, intimidated or harassed.
- Perpetrators of attacks against media personnel and property are brought to justice.
- State and public broadcasters are transformed into truly public service broadcasters as out-lined, among others, in the African Charter on Broadcasting
- Whistleblowers are protected.
- Complaints procedures for aggrieved media professionals exist (e.g. complaint mechanisms of Electoral Management Bodies).

Public authorities should take appropriate steps for the effective protection of journalists and other media personnel and their premises. At the same time this protection should not obstruct them in carrying out their work.

Journalists reporting on the electoral process have a right to be protected from undue pressure and interference from public authorities with a view to influencing the elections and electoral institutions.

At a Zimbabwe conference in November 2022 to mark

the 10th anniversary of the United Nations Plan of Action on the Safety of Journalists, which also coincided with the belated commemoration of the International Day to End Impunity for Crimes Against Journalists, Zimbabwe's Minister of Information, Publicity and Broadcasting Services, Senator Monica Mutsvangwa, said Zimbabwe was "committed to providing a safe operating media environment to enable media practitioners to conduct their duties freely. "I categorically say impunity on crimes against journalists is unacceptable as it seeks to silence voices that keep our society in check," she said.

MISA recommended that if Zimbabwe domesticated the UN Plan of Action into its national legal framework, this would go a long way in legislating against crimes against journalists and thereby limiting cases of abuse by officials because of the risk of prosecution for criminal acts against media practitioners.

The Danger of "Fake News"

The world is battling with a phenomenon largely known by the shorthand term, "Fake News". The term is a summary of three problems — misinformation, disinformation and malinformation— which have created an "information disorder" where the public and the media must be wary of their sources of information, and need to verify the authenticity of the information or risk spreading false information.

In the age of "fake news", journalists need special training in rigorous fact-checking and information verification ahead of elections.

What is fact-checking?

This is a systematic process of investigating claims or information in order to verify facts. Fact-checking often focuses on claims by public officials and institutions. However, because the internet revolution has made anyone with access to the internet a potential publisher, fact-checking needs to be extended to user generated content as well.

It is, however, important to note that fact-checking does not assess the truthfulness of opinions and predictions, hyperbole, satire and jokes.

Promoting factual reporting

A fact is something that is consistent with objective reality or that can be proven with evidence. The usual test for a statement of fact is verifiability — that is whether it can be demonstrated to correspond to experience. Standard reference works are often used to check facts.

As a discipline, fact-checking is only concerned with verifiable facts, not opinions, predictions, jokes and satire - that is humorous dramatising of issues and presentation of information.

The fight against “fake news”

Fact-checking is often defined as the fight against ‘fake news.’

But what constitutes ‘fake news’?

Fake news is information that has been deliberately fabricated and disseminated with the intention to deceive and mislead others into believing

falsehoods or doubting verifiable facts. It is disinformation that is presented as, or is likely to be perceived as, news. - Ethical Journalism Network

The phrase 'fake news' is also broadly used to describe untruths that are frequently (deliberately or unwittingly) shared on various social media platforms, especially Facebook, YouTube, Instagram and Twitter as well as widely used messaging applications such as WhatsApp.

Information Disorder

According to UNESCO, these untruths can be broken down into the following:

- Disinformation: Information that is false and deliberately created to harm a person, social group, organisation or country.
- Misinformation: Information that is false but not created with the intention of causing harm
- Mal-information: Information that is based on reality, used to inflict harm on a person, social group, organisation or country.
- This could take the form of satire and parody, click-bait headlines, misleading captions, visuals or statistics, as well as the genuine content that is shared out of context, imposter content (when a journalist's name or a newsroom logo is used by people with no connections to them), and manipulated and fabricated content.

Fake news is harmful

Fake news undermines democracy and freedom:

- Democracy thrives when people can express

themselves freely when good quality information is available to voters and citizens. Fake news disrupts the information ecosystem.

- Poorly informed voters are unlikely to make good choices during elections. This often leads to the election of incompetent, corrupt governments. The long-term effects of this are the erosion of public confidence in the democratic process as well as the emergence of populist, undemocratic regimes.
- Fake news also tends to deepen divisions and incite violence.

Why fact-checking is important

- Given the evident threat that information disorder (or fake news) is to democracy and social cohesion, there have been attempts to combat this phenomenon using regulation.
- Some undemocratic governments have also sought to use the emergence of 'fake news' as
- an excuse to stifle media freedom and free expression.
- The regulation route poses obvious risks to democracy.
- A more effective way of fighting the information disorder is by equipping citizens with the tools
- they can use to evaluate the information they receive.
- This is why fact-checking is vital.

Basic Fact-checking steps

1. Who said it?
2. Verify with other sources

3. When: check the dates. What is the context – is it new?
4. Check your own biases. We believe what we already believe.
5. Ask experts.

For images/videos

Check the photograph or video to verify if the visual data matches with the supplied details, for things like:

Signage; Language (on billboards, T-shirts, food packaging); flags or emblems); license plates on cars; where is the driver's seat placed; geographical features; architectural features and visible weather conditions. Many false images are circulated during elections for propaganda and campaign purposes, and journalists should acquire skills to detect them, including through reverse image searches for images.

Propaganda and Electioneering

Rival Zimbabwean political parties and allied supportive structures are heavily invested in election propaganda involving massive disinformation, mal-information and misinformation.

Journalists and media houses stand a huge risk of getting sucked and sullied by the propaganda and electioneering campaigns if they disseminate information from the competing parties and their supporters without verifying it.

Essential guidelines

Respect for truth and for the right of the public to truth is the first duty of the journalist.

In pursuance of this duty, the journalist shall at all times defend the principles of freedom of expression in the honest collection and dissemination of news and the right to fair comment and criticism.

Check and recheck-check and recheck the facts to avoid being sold dummies by those with hidden agendas.

Be wary of devious politicians for they will go to any lengths to discredit their opponents in order to get into power.

Search for new voices, views and comments and explanations from diverse news sources. The journalist shall not suppress essential information or falsify documents.

The journalist shall do the utmost to rectify any published information which is found to be harmfully inaccurate.

The journalist shall observe professional secrecy regarding the source of information obtained in confidence.

The journalist shall not be the purveyor of discrimination based on race, gender, sexual orientation, tribe, ethnicity, language, religion or political affiliation.

Never compromise on professional integrity. Journalists' stock in trade should be anchored in the codes and ethics of the profession as espoused by various media houses, media representative and media development

organisations such as MISA Zimbabwe, Voluntary Media Council of Zimbabwe (VMCZ), Zimbabwe Union of Journalists (ZUJ), Media Monitors Zimbabwe), Gender and Media Connect (GMC) and Zimbabwe National Editors Forum (ZINEF).

Above all, journalists should make it their cardinal rule to report both sides of the story by detailing the account of an event through the inclusion of as many voices to authenticate the story thereby assisting the public in coming up with balanced views on events that shape their daily lives and how they can best deal with the issues at hand.

The Guidelines on Media Coverage of Elections in the SADC Region further stress that it is vital to:

- a. Ensure that journalists are familiar with the national legislative framework governing the electoral process and are fully conversant with all aspects of the electoral process, including the electoral institutions;
- b. Be familiar with regional and continental principles and benchmarks on election coverage;
- c. Provide platforms for accessing information that enable informed analysis and opinion on elections.

The role of the media is to report the entire electoral process:

Pre-voting

- Electoral management institutions
- Civic education
- Electoral system

- Demarcation of constituencies
- Voter registration
- Voters' roll
- Candidate or party registration
- Nomination processes
- Official campaign period

Voting Period

- Voting days
- Voting procedures
- Location of polling stations
- Activities at polling stations
- Role of stakeholders at polling stations
- Election monitors
- Election observers and their observations
- Vote counting and results

Post Voting Period

- Appointments to office
- Analysis of promises made by the government/
governing party
- Holding parties accountable.

Grave professional offences

- Plagiarism
- Malicious slander, libel and unfounded accusations
- Acceptance of bribes in any form in consideration of
either publication, broadcast or suppression.

Elections in Zimbabwe

In Zimbabwe, elections are regulated by the Constitution of Zimbabwe as well as the Electoral Act. Chapter 7 of the Constitution outlines electoral principles that Zimbabwe should adhere to, while Part 2 of Chapter 12 of the Constitution establishes an Independent Zimbabwe Electoral Commission (ZEC), which is tasked with the running of Zimbabwe's electoral process. ZEC's obligations include, but is not limited to the demarcation of constituency and ward boundaries and registration of voters.

The obligations extend to the accreditation of journalists covering Zimbabwean elections and monitoring the conduct of the media during the elections.

Besides responsibility to provide voter education, ZEC also monitors voter education provided by other organisations such as the Zimbabwe Election Support Network (ZESN) for correctness and impartiality.

Rights to Voter's Roll

The law states that the voters' rolls should be more accessible to the public and that ZEC shall provide copies of rolls at cost to candidates and political parties, in both print and electronic versions.

ZEC is required to provide a sufficient number of conveniently situated polling stations and to allow input from political parties on their location. After counting of votes at polling stations, results to be

displayed to candidates and agents and posted outside polling stations before being transmitted to constituency centre.

Recounting votes

ZEC has power to order recount of votes, either on request by party or candidate or on its own initiative.

Under the new legislation, ballot papers will be destroyed 14 days after election unless an election petition is lodged.

Media conduct during elections is also governed by the Zimbabwe Electoral Commission (Media Coverage of Elections) Regulations (Statutory Instrument 33 of 2008). The regulations require equitable coverage of political parties by both print publishers and broadcasters.

In the case of broadcasters, the regulations set conditions on the allocation of airtime for defined programmes as well as the conduct of presenters and journalists. The instrument criminalises the use of hate speech and use of inflammatory statement. The spirit of the regulations is to create a peaceful electoral environment.

Encouragement to violence, racial, ethnic and religious hatred is forbidden. ZEC is mandated to monitor the media to ensure observance of this provision.

Zimbabwe Electoral Commission

ZEC is the election management body entrusted with the conduct of elections and to direct and control the registration of voters. It is also responsible for providing voter education.

Polling Stations/Presiding Officers

The Presiding Officer is the key person at any polling station and is in charge of all the administrative and polling process at a polling station. Journalists are not allowed inside a polling station unless casting a vote.

When you visit a polling station you should introduce yourself to the presiding officer. With the permission of the officer, you may be allowed to take pictures and conduct interviews as well as observe proceedings.

Resources:

Media + Elections, A Reporting Handbook

https://en.unesco.org/sites/default/files/media_elections_and_elections_reporting_handbook_en.pdf

AFP Editorial Standards and Best Practices

https://www.afp.com/communication/chartes/12_april_2016_afp_ethic_final.pdf

<https://www.unesco.org/en/articles/unesco-publishes-new-handbook-media-and-elections-during-era-social-media-and-ai>

<https://zimfact.org>



ALERT BUTTON ANDROID APP



Download on Google play store.
or from the MISA Website
<https://tinyurl.com/misabutton>

