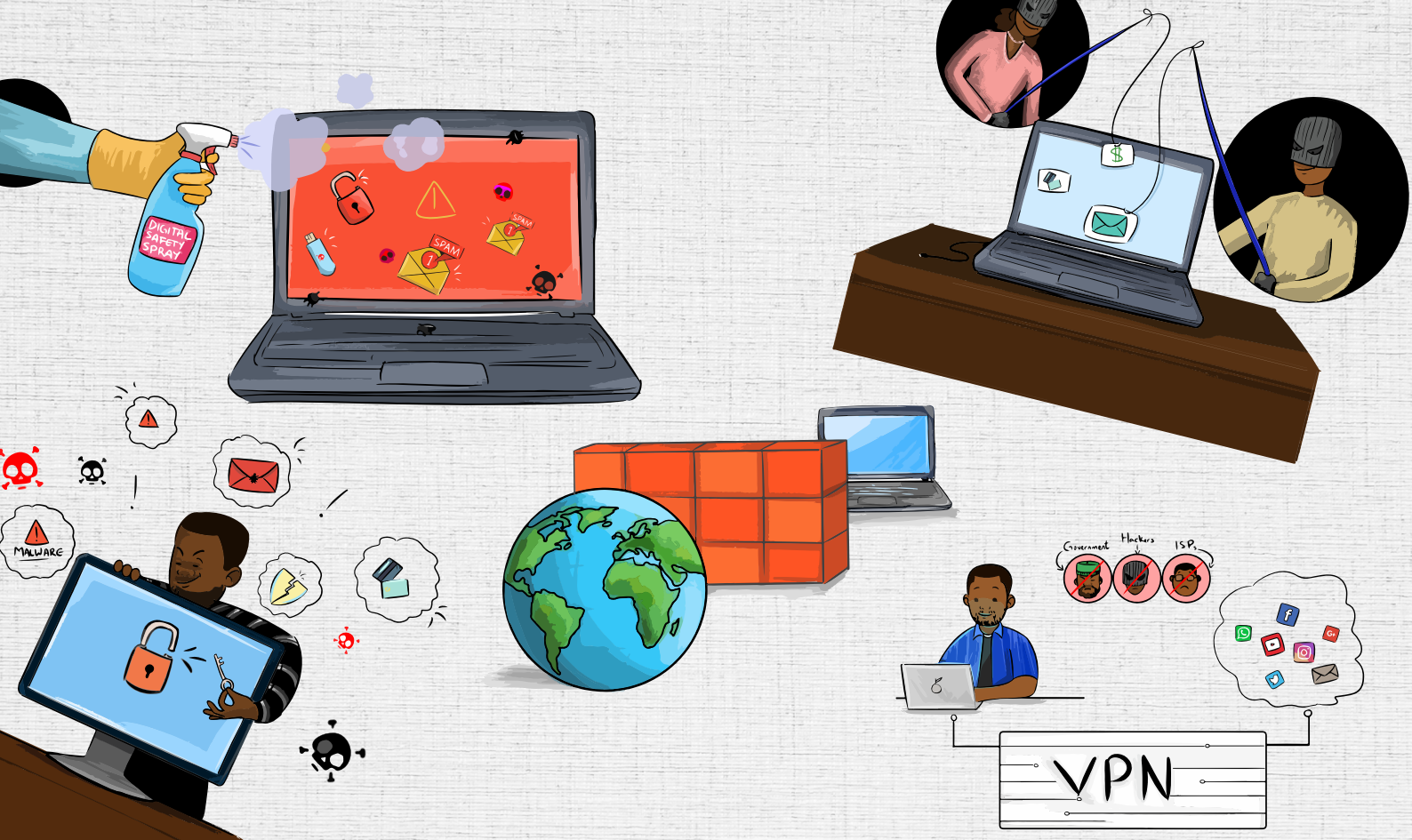
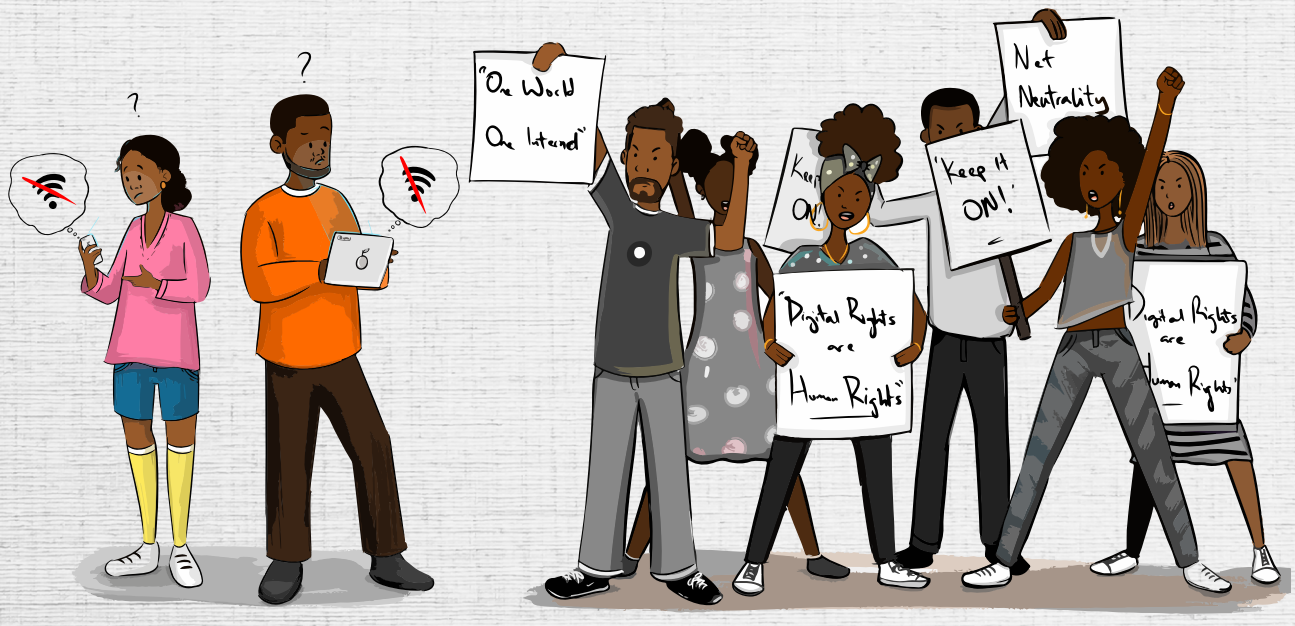


AYETA

Digital Rights Toolkit



Kingdom of the Netherlands

PARADIGM INITIATIVE

Stanford PACS
Center on Philanthropy and Civil Society
Digital Civil Society Lab

FOREWORD

As digital rights advocates increasingly become concerned about their digital security, it is critical that they take measures to protect themselves while in the line of duty. This toolkit provides digital security tips and measures that can be taken against potential threats. It also includes profiles of digital security actors, a calendar of relevant digital rights events on the continent, and last but not the least, the links to resources such as digital security case studies from selected African countries, model policy briefs and media releases, and model coalition statements. A section of the toolkit is dedicated to network disruptions, what you can do to circumvent, how to keep records, and advocacy resources for such moments.

The toolkit was developed as a 2020 Stanford Digital Civil Society Fellowship project, with additional support from the Netherlands Human Rights Fund. 'Gbenga Sesan and Bonface Witaba led project coordination, curriculum development, writing and editing, with support from the Paradigm Initiative team. English proofreading and copy-editing was done by Fisayo Alo. Special thanks to Ashnah Kalemera (CIPESA), Berhan Taye (AccessNow), Demba Kandeh (School of Journalism & Digital Media, University of The Gambia), Ephraim Kenyanito (Article 19 UK), Koliwe Majama (AfDEC), Liz Orembo (KICTANet), Neema Iyer (Pollicy), Neil Blazevic, Oluwatosin Alagbe (PTCIJ), Oyinkansola Akintola-Bello (Co-creation Hub), Ronald Kekembo (FrontlineDefenders) and Vivian Affoah (Media Foundation for West Africa) for reviewing the first version of the toolkit. Your generous feedback has helped us improve the current version.

The toolkit is designed with the overarching aim of addressing the growing need to safeguard digital rights defenders, journalists, whistle blowers, and others working with sensitive information in the global South. Paradigm Initiative (PIN) is dedicated to making the toolkit user friendly and ensuring it remains a living resource by making newer versions available. We rely on your feedback – comments, ideas, criticism, and stories to achieve this. Please send feedback to *hello@ayeta.africa*

TABLE OF CONTENTS

Chapter I

Digital Rights

1.1 Background

The advent of the Internet and its subsequent opening up to the world in 1989, has witnessed human rights defenders innovating in their use of the online spaces to advance the freedom of expression, the freedom of association online, as well as enhance the capacity of a digital society. The Internet today is viewed as a social good, connecting more than half the world. However, it has increasingly become more volatile and on the rise are incidences of challenges posed to activists, human rights defenders, dissidents, and journalists. Authoritarian regimes have resorted to using digital tools and tactics such as Internet shutdowns, online censorship, and digital surveillance to clamp down on free expression.

Figure 1: African Characters Championing Digital Rights

As documented in Paradigm Initiative's 2019 Digital Rights in Africa report,[1] "Over the past decade, there has been an increase in the impact of African organizations championing digital rights - affordable and quality Internet connectivity, privacy, freedom of opinion, expression and association, amongst others. In sharp contrast to this renaissance of digital rights amongst citizens on the continent, the vision of African governments regarding the role of Internet connectivity and digital access to the continent has largely been about retaining political power and control by all means. The overwhelming instinct has been largely toward subordinating rights and access in order to retain political control over citizens."

A 2019 CIPESA report reveals that up to 22 African governments had ordered network disruptions in the last four years and that since the start of 2019, 6 African countries – Algeria, the Democratic Republic of Congo (DR Congo), Chad, Gabon, Sudan and Zimbabwe – had experienced internet shutdowns, while others have experienced some form of information controls measures.[2] The actions of these countries directly contravene the African Declaration on Internet Rights and Freedoms (AfDec) Principles,[3] as well as the Universal Declaration of Human Rights (General Assembly resolution 217 A).[4]

1.2 What are digital rights?

Digital rights are basically human rights in the Internet era. The rights to online privacy and freedom of expression, for example, are really extensions of the equal and inalienable rights laid out in the United Nations Universal Declaration of Human Rights.[5] Digital rights pertain to the rights of individuals to computer access and the ability to use and publish digital contents. It refers to the allowed permissions to fair use of digital materials and the right to privacy. According to the UN, disconnecting people from the Internet violates these rights and goes against international law.[6]

1.3 Digital/Human Rights Charters, Declarations and Protocols

Digital rights and Human rights must be synced so that existing human rights principles are translated to the Internet environment and across the spectrum of Internet policy-making domains.

1. UN Declaration of Human Rights

1 https://paradigmhq.org/download/dra19/
2 https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/
3 https://africaninternetrights.org/articles/
4 http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217%28III%29
5 http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217%28III%29
6 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

The Universal Declaration of Human Rights (UDHR) is a milestone document in the history of human rights. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) as a common standard of achievements for all peoples and all nations. It sets out, for the first time, the fundamental human rights to be universally protected and it has been translated into over 500 languages.[7]

2. African Charter on Human and People's Rights

The African Charter on Human and Peoples' Rights (also known as the Banjul Charter) is an international human rights instrument that is intended to promote and protect human rights and basic freedoms in the African continent. The Charter was adopted on June 1 1981, and came into force on October 21 1986. The Charter establishing the Organisation of Africa Unity (OAU) imposed no explicit obligation on member states for the protection of human rights, it however, required states parties to have due regard for human rights as set out in the Universal Declaration of Human Rights in their international relations.[8]

3. African Declaration on Digital Rights

The African Declaration on Internet Rights and Freedoms is a Pan-African initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation on the continent. The Declaration is intended to elaborate on the principles which are necessary to uphold human and peoples' rights on the Internet, and to cultivate an Internet environment that can best meet Africa's social and economic development needs and goals. The Declaration builds on well-established African human rights documents including the African Charter on Human and Peoples' Rights of 1981 the Windhoek Declaration on Promoting an Independent and Pluralistic African Press of 1991 the African Charter on Broadcasting of 2001, the Declaration of Principles on Freedom of Expression in Africa of 2002 and the African Platform on Access to Information Declaration of 2011.[9]

4. African Union Declaration of Principles on Freedom of Expression and Access to Information in Africa

The Declaration of Principles on Freedom of Expression in Africa was adopted in 2002 by the African Commission on Human and Peoples' Rights. The document serves as a reference point for assessing African countries' records at the Commission. It has also been a strong reference point for jurisprudence in Africa.[10]

5. African Union Declaration on Internet Governance

7 https://www.un.org/en/universal-declaration-human-rights/
8 https://au.int/en/treaties/african-charter-human-and-peoples-rights
9 https://africaninternetrights.org/about/
10 https://www.achpr.org/public/Document/file/English/draft_declaration_of_principles_on_freedom_of_expression_in_africa_eng.pdf

The African Union Declaration on Internet Governance was developed through a consultative process in order to accrue the benefits of the digital economy by creating a conducive and an enabling environment for African stakeholders to come together, deliberate critical emerging issues and contribute to the development of Internet public policies that take into account the needs of Africa. The Declaration acts as the guiding principles for stakeholders and constitutes the shared values and pillars that all can agree on and build upon during future deliberations and debates on the future of the Internet from an African standpoint.[11]

6. ECOWAS Protocol on Democracy and Good Governance

The ECOWAS Protocol on Democracy and Good Governance was adopted in December 2001 by the Heads of State and Government as supplementary to the Protocol relating to the Mechanism for Conflict Prevention, Management, Resolution, Peacekeeping and Security (1999).[12]

1.4 Digital Security Actors

Figure 2: Digital Security Actors

11 https://au.int/sites/default/files/newseventsworkingdocuments/33025-wd- african_declaration_on_internet_governance_en_0.pdf
12 https://www.ohchr.org/EN/Issues/RuleOfLaw/CompilationDemocracy/Pages/ECOWASProtocol.aspx

Many digital security actors have various initiatives to mitigate the vulnerabilities and risks of journalists and human rights advocates. These organisations may be contacted for advice and/or assistance with matters related to data breaches, incidence reporting, and policy issues etc.

1. **AccessNow - https://www.accessnow.org/**
   AccessNow provides round the clock digital security helpline, evidence-based policy analysis, advocacy and grants to grassroots organizations and activist groups that are working with users and communities most at risk of digital rights violations.

2. **AfricanDefenders - https://africandefenders.org/**
   A pan-African human rights defenders network of five African sub-regional organisations, dedicated to the promotion and protection of human rights defenders (HRDs) across the African continent.

3. **Africtivistes - https://www.africtivistes.org/**
   A pan-African network of online activists and bloggers for democracy, comprising a community of 200 cyber-activists from 35 different countries.

4. **Association for Progressive Communication (APC) - https://www.apc.org/**
   The APC works to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies.

5. **Association of Media Women in Kenya (AMWIK) - http://amwik.org/**
   The AMWIK is a national media association with focus on enhancing the visibility of women in the society and promoting their participation in leadership and decision-making.

6. **Article 19 - https://www.article19.org/**
   Article 19 – working on two interlocking freedoms: the Freedom to Speak, and the Freedom to Know, – seeks to make people everywhere express themselves freely and actively engage in public life without fear of discrimination.

7. **Cc-Hub - https://cchubnigeria.com/**
   Commonly referred to as Cc-HUB or the HUB, it is a platform where technology-oriented people share ideas on solving social problems in Nigeria.

8. **Central Africa Human Rights Defenders Network (Réseau des Défenseurs des Droits Humains en Afrique Centrale – REDHAC) - https://defenddefenders.org/africandefenders/**
   This human rights Central African based organisation accompanies and reinforces the work of human rights defenders (HRDs) with the aim to mitigate their vulnerabilities and risks, and raise awareness on the human rights situation in Central Africa.

9. **Collaboration on International ICT Policy in East and Southern Africa (CIPESA) - https://cipesa.org/**
   Based in Kampala, Uganda, CIPESA is an Internet policy organization working in East and Southern Africa to promote effective and inclusive ICT Policy in Africa.

10. **Committee to Protect Journalists (CPJ) - https://cpj.org/**
    An American independent not-for-profit, non-governmental organization, based in New York City, with correspondents around the world. CPJ promotes press freedom and defends the rights of journalists around the world.

11. **Cyber Security Africa - https://www.cybersecurityafrica.com/**
    A full-service Information Security Consulting firm offering a comprehensive range of services and products to help organizations protect their valuable assets.

12. **Defend Defenders - https://defenddefenders.org/**
    Poised for protecting and promoting human rights defenders in the East and Horn of Africa sub-regions.

13. **Digital Security Alliance (DSA) – https://defendersprotection.org/the-digital-security-alliance/**
    A coalition of organisations and individual digital security experts working towards securing the digital assets of the civil society, human rights defenders, journalists and other activists in the face of threats posed by powerful corporations, unscrupulous criminals, the state and other non-state actors.

14. **Freedom House - https://freedomhouse.org/**
    A U.S.A-based not-for-profit, non-governmental organization that conducts research and advocacy on democracy, political freedom, and human rights.

15. **Frontline Defenders - https://www.frontlinedefenders.org/**
    An Irish-based human rights organisation founded in Dublin, Ireland in 2001 to protect those who work non-violently to uphold the human rights of others as outlined in the Universal Declaration of Human Rights.

16. Gambia Cyber Security Alliance - http://gamcybersecurityalliance.com/

The Gambian based organisation aims to create awareness and increase understanding of Gambians about cyber security, cyber threats, espionage, and empowering them to be safer and more secure online.

17. Gambia Press Union - http://www.gambiapressunion.org/our-work/

The Gambia Press Union is a trade union for journalists in the Gambia, established in 1978 by a group of journalists, with a mission to foster a free and vibrant media.

18. Human Rights Defenders Network - Sierra Leone (HRDN-SL) https://namati.org/network/organization/pan-african-human-rights-defenders-network/

HRDN-SL is a coalition of human rights civil society organizations and individuals working for the protection and promotion of human rights in Sierra Leone. It was established as a local chapter of the Pan African Human Rights Defenders Network (PAHRDN) based in Uganda and the West Africa Human Rights Defenders Network (WAHRDN) based in Togo with technical support from the International Service for Human Rights (ISHR) based in Geneva.

19. Kenya ICT Action Network (KICTANET) - https://www.kictanet.or.ke

A multi-stakeholder Think Tank for stakeholders interested and involved in ICT policy and regulation. Its work is guided by four pillars of Policy Advocacy, Capacity Building, Research, and Stakeholder Engagement. KICTANET doubles as a space for translating the ideas given by listers into meaningful proposals for resolution of challenges facing the ICT sector.

20. Media Foundation for West Africa (MfWA) - https://www.mfwa.org/

Established in 1997 and based in Accra, Ghana, MfWA is a regional non-governmental organisation to promote and defend the right to freedom of expression of all persons particularly the media and human rights defenders in West Africa.

21. Media Legal Defense Initiative (MLDI) - https://www.mediadefence.org/

A non-governmental organization established in 2008 to provide legal assistance to journalists and independent media. It also supports training in media law and promotes the exchange of information, litigation tools and strategies for lawyers working on media freedom cases.

22. National Coalition of Human Rights Defenders – Kenya (NCHRD-K) - https://defenderscoalition.org/

A national organization incorporated in the Republic of Kenya as a Trust. Its mission is

to strengthen the capacity of human rights defenders (HRDs) to work effectively in the country and to reduce their vulnerability to the risk of persecution.

23. Paradigm Initiative (PIN) - https://paradigmhq.org/

Paradigm Initiative is a social enterprise that builds an ICT-enabled support system and advocates for digital rights in order to improve livelihoods for under-served youth. PIN's digital rights advocacy program is focused on the development of public policy for internet freedom in Africa.

24. Pollicy - https://pollicy.org/

Pollicy is a technology consulting and development firm aimed at improving government service delivery through improved civic engagement and participation.

25. Safe Sisters - https://safesisters.net/

Safe Sisters is a fellowship program for women human rights defenders, journalists or media workers, and activists. Fellows are trained to be able to understand and respond to the digital security challenges they face in their work and daily life.

26. Women Human Rights Defenders (WHRD) - https://www.peacewomen.org/

Women Human Rights Defenders (WHRD) are both female human rights defenders, and any other human rights defenders who work in the defense of women rights or on gender issues.

27. Women of Uganda Network (WOUGNET) - https://wougnet.org/

WOUGNET was founded in May 2000. The organisation is dedicated to aiding women and women's organizations in the use of information and communication technologies, focusing on use of mobile phones, e-mail and the web, as well as the integration of "traditional means" such as radio, video and print in a way that enables wider outreach.

1.5 Relevant Digital Rights Events

Annually, across Africa, a number of digital rights and security events are organized and the events bring together stakeholders from different backgrounds, to discuss policy issues, emerging trends, and offer hands-on training.

Figure 3: Relevant Digital Rights Events

1. **African School on Internet Governance (AfriSIG):**
   A multi-stakeholder training initiative that aims to give Africans the opportunity to gain knowledge and confidence to participate effectively in internet governance processes and debates nationally, regionally and globally. https://www.apc.org/en/project/african-school-internet-governance-afrisig

2. **Cc-HUB Digital Security Demo Day:**
   Businesses, civil society, students and information security enthusiasts from within and outside Lagos converge to witness live cyber-attacks and countermeasures. https://cchubnigeria.com/cchub-hosts-first-cybersecurity-conference/

3. **Digital Rights and Inclusion Forum (DRIF):**
   DRIF is a bi-lingual forum hosted every April by Paradigm Initiative, where tough topical

global issues around Internet rights, especially in Africa, are discussed between civil society, technology companies, government, academia and other stakeholders. https://drif.paradigmhq.org/

4. **East Africa Cyber Security Convention:**
   The East Africa Cyber Security Convention seeks to equip participants with knowledge on how to mitigate Cyber Security threats. https://cloudsecurityalliance.org/csa_events/east-africa-cyber-security-convention/

5. **Forum on Internet Freedom in Africa (FIFAfrica):**
   Hosted annually in September, by CIPESA, it focuses on promoting a Free and Open Internet in Africa. https://cipesa.org/fifafrica/

6. **Regional Initiatives / Schools of Internet Governance**
   East Africa School of Internet Governance (EASIG)
   West Africa School of Internet Governance (WASIG)

7. **National Initiatives / Schools of Internet Governance**
   Kenya School of Internet Governance (KeSIG)
   Nigeria School of Internet Governance (NSIG)
   South Sudan School of Internet Governance (SSSIG)
   Tanzania School of Internet Governance (TzSIG)
   Arusha Women School of Internet Governance (AruWSIG)

1.6 Digital Rights Case Studies

The attempts by the state to violate the rights of journalists and digital rights defenders by legislation, internet shut down, and court actions amongst other means are brought to the fore with selected cases (see links) in Cameroon, Nigeria, Tanzania and Zimbabwe.

https://tinyurl.com/y5p57qkw
https://tinyurl.com/y3fedl7f
https://tinyurl.com/y324dmeu
https://tinyurl.com/y63gbr3m

1.7 Model Policy Briefs

The roles of Digital rights advocates, journalists and other social activists are better appreciated when they are seen to contribute to providing solutions to the myriad challenges facing the society. The following links show few policy briefs in this direction.

https://tinyurl.com/y2ynk6oc
https://tinyurl.com/y3r9t974
https://tinyurl.com/y2v9ucfl

1.8 Model Coalition Statements

The rise within African governments' circles to regulate the use of social media through overarching draft legislation with broad terms serve to decrease the openness of the internet, mask human rights violations, and create barriers to long-term stability and peaceful dialogue. The ability to stand off to this tendency is strengthened when stakeholders come together with a single voice. Few examples of coalition statements made to address related issues are examined in the following links.

https://tinyurl.com/yyt8kkhp
https://tinyurl.com/y5eku8et
https://tinyurl.com/y4l6lwkg
https://tinyurl.com/y38k8mut

Chapter II

2.1 Digital Safety and Security

Digital safety, interchangeably referred to as Internet safety, online safety and or Cyber safety refers to an array of practices and precautions adhered to by an individual when using the Internet, in efforts to ensure that sensitive personal information and that of their device(s) remains secured.

a. How to stay protected online

According to an updated "What happens in an Internet minute" 2020 infographic, 190 million mails, 194,444 tweets, 19 million WhatsApp texts happen every 60 seconds. With ITU statistics indicating that over 4.5 Billion people (50%) of the world population is connected online, this could only mean that more bad actors, hackers, threats and online scams lurk more than ever before. To guarantee digital safety of journalists, digital rights defenders and other Internet users, an array of digital hygiene considerations need to be adhered to, to help curb digital security threats and incidents.

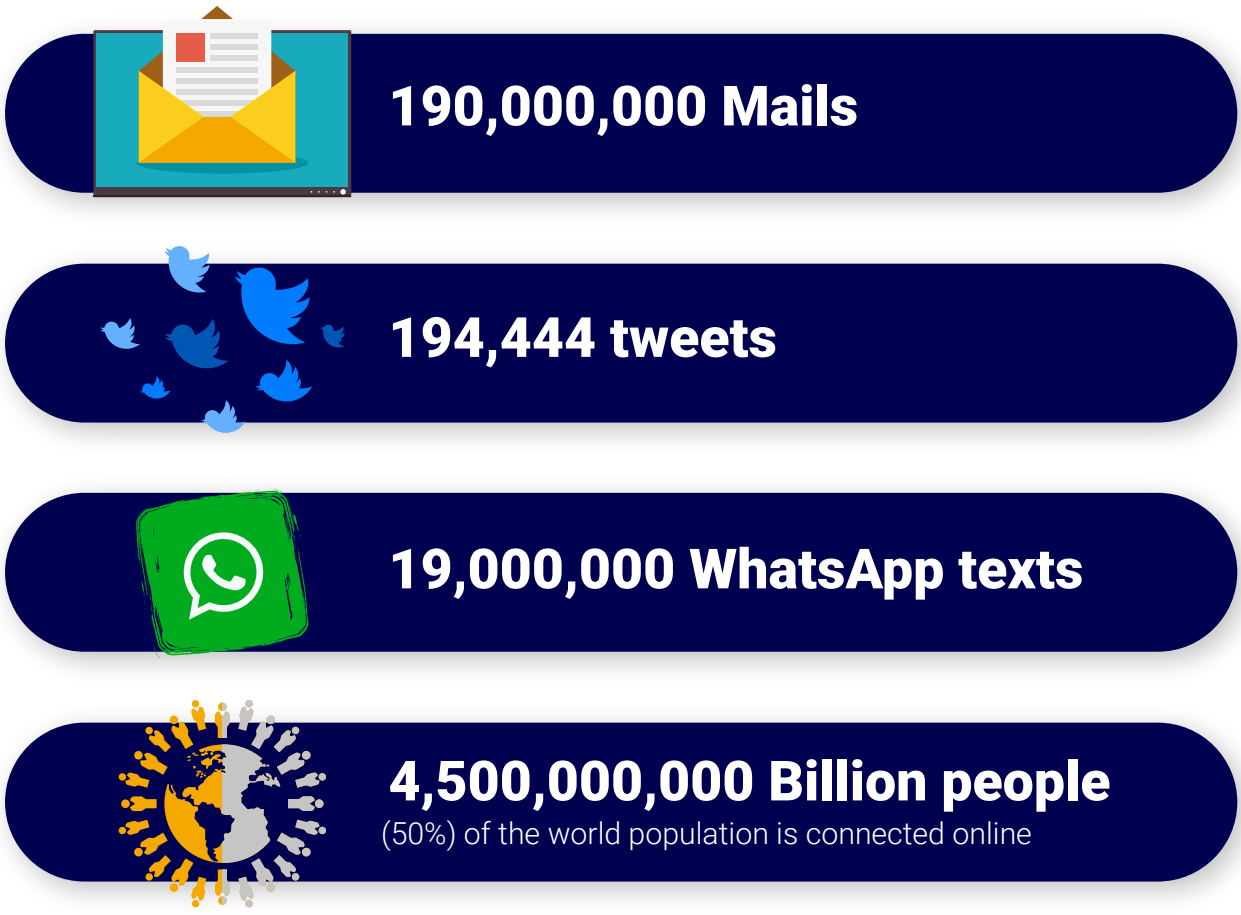


Figure 4: What happens in an internet minute

b. Digital Hygiene

Digital hygiene is the catch-all term for the practices and behaviours related to cleaning up and maintaining our digital world. This includes everything from organizing the files on your PC, to locking down your social media accounts, to introducing new apps or technologies to make your digital life easier or more secure. We might hear this being called cyber hygiene or Internet hygiene—these all really mean the same thing.

Figure 5: Digital Safety and hygiene

c. Benefits of Digital Hygiene

By safeguarding the information you share online and or securing the devices you use, you reduce both the likelihood of getting attacked and the severity of a successful attack. Whatever you post online can become a source or a piece of information used by a bad actor to launch a scam or cyber-attack against you. As a digital rights actor, maintaining good digital hygiene practices is key in keeping you safe on the Internet.

2.2 Digital Hygiene Practices

Figure 6: Develop Safe Online Habits

a. Develop Safe Online Habits

There are some easy things you can do, without purchasing expensive technology or investing a lot of time in reconfiguring your home network, to make your online computing safer. The list below is a good starting place and connects to other areas of our site to get more detailed information about each security measure.

1. Keep your systems and software up to date.[13]
2. Always have a current/updated anti-virus running.[14]
3. Avoid phishing scams.[15]
4. Use a complex password or a password manager.[16]
1. Be careful what you click; a disreputable website can link you to cyber criminals and bad actors.
2. Never leave your computer or devices unattended. Lock any screens when you head to the restroom. An open system is an open invitation to your data.
3. Create a pin for your mobile device, and try to never leave it on in an airplane.[17]
4. Protect your data.
5. For all personal files, backup your data! You never know when you may lose your hard drive, and if the data will be recoverable. There are many cloud storage options, an external drive is also an option.[18]
6. When shopping online, or sharing sensitive data, be sure you are sending information encrypted by looking for “https” or the lock icon in your address bar.
7. Be smart about what you share (and don’t share) on social media.[19]
8. In the physical world, be careful of social engineering. This can be an attempt by a strangerto pull information from you that you wouldn’t share online. Birthday? Favorite vacation spot? First pet’s name? Do they really need that information? The answers to these questions may result in compromised accounts.
9. Be sure to monitor your financial and social media accounts for suspicious activity.[20]

b. Passwords & Authentication

If you are looking for a way to improve your cyber security, password security is where you should start. Ideally, a password is a basic security mechanism that consists of a secret passphrase created using alphabetic, numeric, alphanumeric and symbolic characters, or a combination. This security mechanism is used to restrict access to a system, application or service to only those users who have memorized or stored and/or are authorized to use it. The standard digital safety practice involves creating strong passwords, not reusing

13 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/updates-patching
14 https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/anti-virus
15 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/phishing
16 https://cybersecurity.osu.edu/cybersecurity-you/passwords-authentication/passwords
17 https://cybersecurity.osu.edu/cybersecurity-you/protect-personal-devices/mobile-devices
18 https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/file-backups
19 https://cybersecurity.osu.edu/cybersecurity-you/develop-safe-habits/file-backups
20 https://cybersecurity.osu.edu/about/teams/identity-access-management

passwords, using passphrases and multi-factor authentication, carefully considering password reset questions, not writing down passwords, and last but not least, using a password manager.

c. Password generators

A password generator is a software tool that creates random or customized passwords for users. It helps users create stronger passwords that provide greater security for a given type of access.

d. Importance of Password Generators

Password generators help those who have to constantly come up with new passwords to ensure authorized access for programs and to manage a large number of passwords for identity and access management. Other kinds of tools include a password vault, where users manage large numbers of passwords in a secure location.

e. Passwords Managers

A password manager is a tool that creates and stores passwords so that many different passwords may be used on different sites and services without having to memorize them.
Password managers:

- **Generate strong passwords that a human being would be unlikely to guess.**
- **Store several passwords (and responses to security questions) safely.**
- **Protect all passwords with a single master password (or passphrase).**[21]

KeePassXC is an example of a password manager that is open-source and free. This tool can be kept on the desktop or integrated into a web browser.[22] KeePassXC does not automatically save changes made when using it, so if it crashes after some passwords have been added, they can be lost forever, but this can be changed in the settings. Please note that using password managers is like putting all your eggs in one basket and protecting them with your life. The risk with hacked password managers is that access to the "basket" means access to all your "eggs".

21 https://ssd.eff.org/en/glossary/passphrase
22 https://ssd.eff.org/en/glossary/web-browser

2.3 Common Password Attacks

Figure 7: Secure passwords

a. Trying Common Passwords

One of the easiest and most common ways to hack into an account is to try[23] common passwords or to do a little research on the intended victim and try some passwords related to that person. A 2019 CNN report revealed that the top 10 most commonly-used and hacked passwords were:

1. 123456
2. 123456789
3. qwerty
4. password
5. 111111
6. 12345678
7. abc123
8. 1234567
9. password1
10. 12345

These are VERY insecure passwords. They are easy to guess and cyber criminals will start

23 https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/index.html

trying to access accounts with perceived weak passwords like these.
We also recommend to NEVER use passwords that contain the following information:

- **Your name or the names of your family and friends,**
- **Your birthday or those of your family and friends,**
- **Pets names, and**
- **Places you live or have lived including cities or street names.**

It is amazing how much information about a person is out there on the internet. So if your password contains information that pertains to you in a way that can be discerned from the internet or by talking to your friends, it can be easily guessed.

b. Brute Force Attack

A brute force attack simply tries every possible combination of allowed characters until it finds a match. This kind of attack is very effective on shorter passwords and it will even be able to hack passwords composed of randomized characters. But the length does matter. A brute force attack is not very efficient and if your password is long enough, it may be impractical to hack. Take a look at the table that shows the time it would take to brute force passwords by length and complexity. Keep in mind that this table assumes that the computer can try significantly more than 1000 passwords per second.

Password Length	All Characters	Only Lowercase
***	0.86 seconds	0.02 seconds
****	1.36 minutes	0.46 seconds
*****	2.15 hours	11.9 seconds
******	8.51 days	5.15 minutes
*******	2.21 years	2.23 hours
********	2.10 centuries	2.42 days
*********	20 millennia	2.07 months
**********	1,899 millennia	4.48 years
**********	180,365 millennia	1.16 centuries
**********	17,184,705 millennia	3.03 millennia
**********	1,627,797,068 millennia	78.7 millennia
**********	154,640,721,434 millennia	2,046 millennia

Figure 8: Password Length/Difficulty table

Notice that the time to hack a password increases exponentially with each character added to your password. For a password that consists of randomized characters of all types, the difference between 6, 7, 8 and 9 characters is days, years, centuries and millennia!!! Also notice how much longer it takes to hack a password that contains all types of characters compared to a password of the same length that uses only lowercase characters.

c. Creating and maintaining strong and secure passwords

Reusing passwords is an exceptionally bad security practice. If a bad actor gets hold of a password that you've reused across multiple services, they can gain access to many of your accounts. This is why having multiple, strong, unique passwords is so important. Fortunately, a password manager can help.[24]

d. Creating Strong Passwords Using Dice

There are a few passwords that you should memorize and that need to be particularly strong. These include:

- **passwords for your device**
- **passwords for encryption (like full-disk encryption)**[25]
- **the master password,**[26] **or "passphrase,"**[27] **for your password manager**
- **your email password**[28]

One of the many difficulties when people choose passwords themselves is that people are not very good at making random, unpredictable choices.[29] An effective way of creating a strong and memorable password[30] is to use dice[31] and a word list[32] to randomly choose words. Together, these words form your "passphrase." A "passphrase" is a type of password that is longer for added security. For disk encryption and your password manager, we recommend selecting a minimum of six words.

Why use a minimum of six words? Why use dice to pick words in a phrase randomly? The longer and more random the password, the harder it is for both computers and humans to guess. To find out why you need such a long, hard-to-guess password, here's a video explainer.[33]

If your computer or device gets compromised and spyware is installed, the spyware can watch you type your master password and could steal the contents of the password manager. So it's still very important to keep your computer and other devices clean of

24 https://ssd.eff.org/en/glossary/password-manager
25 https://ssd.eff.org/en/glossary/encryption
26 https://ssd.eff.org/en/glossary/master-password
27 https://ssd.eff.org/en/glossary/passphrase
28 https://ssd.eff.org/en/glossary/password
29 http://people.ischool.berkeley.edu/~nick/aaronson-oracle/
30 https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases
31 https://www.eff.org/dice
32 https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt
33 https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice

malware when using a password manager.

e. Syncing Passwords Across Multiple Devices

Many password managers allow access to passwords across devices through a password-synchronization feature. This means when a password file is synced on one device, it will automatically on all other devices. Password managers can store passwords "in the cloud," meaning encrypted on a remote server. When the passwords are needed, these managers will retrieve and decrypt[34] the passwords automatically. Password managers that use their own servers to store or help synchronize passwords are more convenient, but are slightly more vulnerable to attacks. If passwords are stored both on the computer and in the cloud, an attacker does not need to take over the computer to find out the passwords. (They will need to break the password manager's passphrase though.) If this is concerning, do not sync passwords to the cloud, instead opt to store them on just the devices.

- **Note!**

Keep a backup of the password database just in case. Having a backup is useful if the password database is lost in a system crash, or if the device is taken away. Password managers usually have a way to make a backup file, or one can use the regular backup program.

2.4 Multi-Factor Authentication and One-Time Passwords

Strong, unique passwords make it much harder for bad actors to gain access to digital accounts. To further protect your digital accounts, enable the two-factor authentication.[35] Some services offer two-factor authentication (also called 2FA, multi-factor authentication, or two-step verification), which requires users to possess two components (a password and a second factor) to gain access to their account. The second factor could be a one-off secret code or a number generated by a program running on a mobile device.
Two-factor authentication using a mobile phone can be done in one of two ways:

- **the phone can run an authenticator application that generates security codes (such as Google Authenticator[36] or Authy[37]) or by using a stand-alone hardware device (such as a YubiKey); or**
- **the service can send an SMS text message with an extra security code that is used whenever log in is needed.**

34 https://ssd.eff.org/en/glossary/decrypt
35 https://ssd.eff.org/en/glossary/two-factor-authentication
36 https://support.google.com/accounts/answer/1066447?hl=en
37 https://authy.com/

If you have a choice, pick the authenticator application or stand-alone hardware device instead of receiving codes by text message. It is easier for an attacker to redirect these codes to their own phone than it is to bypass the authenticator. Some services, such as Google, also allow the generation of a list of one-time passwords, also called single-use passwords. These are meant to be printed or written down on paper and carried with you. Each of these passwords works only once, so if one is stolen by spyware when you enter it, the thief will not be able to use it for anything in the future.

a. Multi-Factor Authentication ("MFA")

A Multi-Factor Authentication (MFA) is a security feature offered by many websites, applications and devices that dramatically improves account security. Technically, MFA could refer to a system where there are more than two forms of authentication.

b. How Multi-factor Authentication ("MFA") works

If you have an MFA setup for a given account (website, application or device), when you log in with your username and password that account server is going to ask for a second, independent form of authentication before it will actually let you into the system. It is similar to when a bank account is opened and they ask to see a picture ID and some other form of identification, like the social security card or international passport. It is much harder to pretend you are someone you are not when you have to prove who you are in two different ways!

c. Multifactor Authentication Methods

We recommend registering at least two devices for a multi-factor authentication, so if you lose one device, you can protect yourself by wiping off the data remotely and then use the other device to authenticate. With MFA, the second authentication can be done using one of several different methods so let's take a moment to go over some of the most common ones.

i. Mobile device application "Push" method

The most popular way to get the second form of authentication is through a "push" to an application on your mobile device. There are a variety of authenticator apps that are free and easy to set up and even easier to use for authentication! With this method, the account server that you are trying to log into will send a "push" to your mobile device. This push is a notification that will pop up on the mobile device and say something along the lines of, "Hey, someone is trying to log in to this website, is it you? Should we let them in?" Usually there is a big green button and a big red one so that you can easily answer "Yes" or "No" with one touch. If you hit "Yes", you are in. But if you did not make the original login request, you know that someone has your password and

is trying to log in to your account. You can hit the “No” button and their access will be denied. You can then go log in yourself and change your password so that the attacker is back to square one.
It is simple, yet an extremely effective security measure. The primary advantage of this method is that an attacker not only has to compromise your password, but also has to have physical access to your mobile device and has to be able to log in to that device. The odds that all of that will happen are extremely low. In essence, it is practically zero if you are using decent passwords and you keep track of your phone. Another advantage of this method is that you get a real time notification when someone is trying to illegally log in to your account. As mentioned above, you can use this knowledge to quickly respond by changing your password.

ii. Mobile device application code method

Sometimes the account server will not send you a push but it may ask you to type in a unique code that is generated by the authenticator app on your mobile device. These codes are short (maybe 6 digits) so it may seem like they are not very secure. The cool thing is that the codes are re-generated every minute or so and they are based on an algorithm that is known only to your authenticator app and the account server you are trying to connect to. It would be extremely difficult for a cyber- criminal to right guess the 6 digit code under those circumstances since the time frame is so short. Again, the main advantage here is that the attacker has to have physical access to your mobile device and the ability to log in to it. One downside is that you do not get any real-time notification if someone tries to log into your account. Usually this method is an option as a backup to the push method as well. Most authenticator apps will support both methods.

iii. SMS Code Method

This method also uses your mobile device but it does not use an application. Therefore, it works with non-smartphones. If you set up this method of MFA, when you log in with your username and password, the account server will send your mobile phone a text message with a one-time code. You will then type that code into the website or device portal where you entered your password. This basically has all the advantages of the “push” method, it just isn’t quite as convenient because you have to type in the code. You will get that real-time notification of a login attempt because you will get a text message per attempt. One downside is that an attacker doesn’t necessarily have to be able to log in to your phone. They do have to physically have the phone but text messages often pop up on the screen of the phone even when the phone is locked.

iv. Email Code Method

This method works very much like the SMS code method except that the code is sent to an email account that you have pre-communicated with the account server you are trying to access. You will most often set this up when you register for the multi-factor service you are using. If you're going to use this kind of MFA, you will need to make sure that your email account itself is secure, which probably means that you should have MFA enabled for access to the email account in question. The reason is that email can be checked from anywhere, including the same computer terminal where the cybercriminal is trying to log in to your account. In other words, this method does not require physical access to any independent device. That's why you should have a strong password for your e-mail that is not used anywhere else. If you do that, then this method would essentially require the attacker to know two of your passwords. However, forcing them to have access to another device is a stronger, more secure option. If a website allows only this type of MFA, that is fine. Go ahead and set it up and then require authentication to your mobile device for access to your email. Then you're golden.

v. Physical Token

This method was more popular before the advent of smartphones. A physical "token" is a small device that continuously generates codes in the same way that an authentication app on your mobile device would. It works just as well but it has the added downside that you have to keep track of this other device. These days our lives are tied to our mobile phones. You can imagine the possibility of losing a token and not even realizing it is gone for a while. If you have one of these, keep it in a safe location. If you have to carry it around, maybe attach it to your keychain.

2.5 Two-Factor Authentication ("2FA")

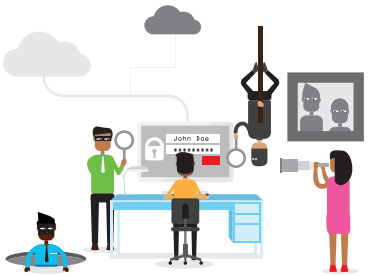
The Two-Factor Authentication (or "2FA") is a type, or subset, of multi-factor authentication, and it is a way to let a user identify him or herself to a service provider by requiring a combination of two different authentication methods. These may be something that the user knows (like a password or PIN), something that the user possesses (like a hardware token or mobile phone), or something that is attached to or inseparable from the user (like their fingerprints).

a. How does 2FA work online?

Several online services – including Facebook, Google, and Twitter – offer 2FA as an alternative to password-only authentication. If you enable this feature you will be prompted for both a password and a secondary method of authentication. This second method is typically either a one-time code sent by SMS or a one-time code generated by a dedicated

mobile app that stores a secret (such as Google Authenticator, Duo Mobile, the Facebook app, or Clef). In either case, the second factor is your mobile phone, something you (normally) possess. Some websites (including Google) also support single-use backup codes, which can be downloaded, printed on paper, and stored in a safe location as an additional backup. Once you've opted-in to using 2FA, you will need to enter your password and a one-time code from your phone to access your account.

Two-Factor Authentication



How does 2FA work online?

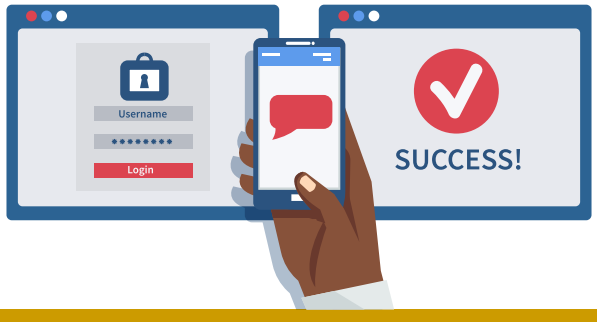
This feature will prompt you for both a password and a secondary method of authentication. This second method is typically either a one-time code sent by SMS or a one-time code generated by a dedicated mobile app that stores a secret.

The second factor is your mobile phone, something you (normally) possess. Once you've opted-in to using 2FA, you will need to enter your password and a one-time code from your phone to access your account.

Why should you enable 2FA?

2FA offers you greater account security by requiring you to authenticate your identity with more than one method.

This means that, even if someone were to get hold of your primary password, they could not access your account unless they also have your mobile phone or another secondary means of authentication.



Are there downsides to using 2FA?

There is an increased risk of getting locked out of your account if, for example, you misplace or lose your phone, change your SIM card or travel to a country without turning on roaming. Using 2FA means you may be handing over more information to a service than you are comfortable with. Suppose you use Twitter, and you signed up using a pseudonym. Even if you carefully avoid giving Twitter your identifying information, and you access the service only over Tor or a VPN, as long as you enable SMS 2FA, Twitter will necessarily have a record of your mobile number. That means if compelled by a court, Twitter can

Figure 9: How does 2 Factor Authentication work?

b. Why should you enable 2FA?

2FA offers you greater account security by requiring you to authenticate your identity with more than one method. This means that, even if someone were to get hold of your primary password, they could not access your account unless they also have your mobile phone or another secondary means of authentication.

c. Are there downsides to using 2FA?

Although 2FA offers a more secure means of authentication, there is an increased risk of getting locked out of your account if, for example, you misplace or lose your phone, change your SIM card[38] or travel to a country without turning on roaming. Similarly, using 2FA means you may be handing over more information to a service than you are comfortable with. Suppose you use Twitter, and you signed up using a pseudonym.[39] Even if you carefully avoid giving Twitter your identifying information, and you access the service only over Tor or a VPN[40], as long as you enable SMS 2FA, Twitter will necessarily have a record of your mobile number. That means if compelled by a court, Twitter can link your account to you via your phone number. This may not be a problem for you, especially if you already use your legal name on a given service, but if maintaining your anonymity is important, think twice about using SMS 2FA.

d. Universal factor authentication

Universal authentication, also known as single sign-on (SSO), is a network identity-verification method that allows users to navigate from site to site securely without having to enter identifying information multiple times. With universal authentication, a subscriber enters one set of parameters (such as a username and password) at the start of every network session. The authentication data for any site visited thereafter is automatically generated for the duration of that session. One of the biggest challenges with Internet security is the fact that every Web site has its own authentication system. A typical Internet user, who has two or three Web-based e-mail addresses and frequents half a dozen online vendors to buy or sell things, must memorize several usernames and passwords. This can be difficult unless the authentication data is written down or stored as a text file, which then becomes a security issue. Universal authentication can eliminate this problem without compromising security or privacy.

38 https://ssd.eff.org/en/glossary/sim-card
39 https://ssd.eff.org/en/glossary/pseudonym
40 https://ssd.eff.org/en/glossary/vpn

2.6 Firewalls

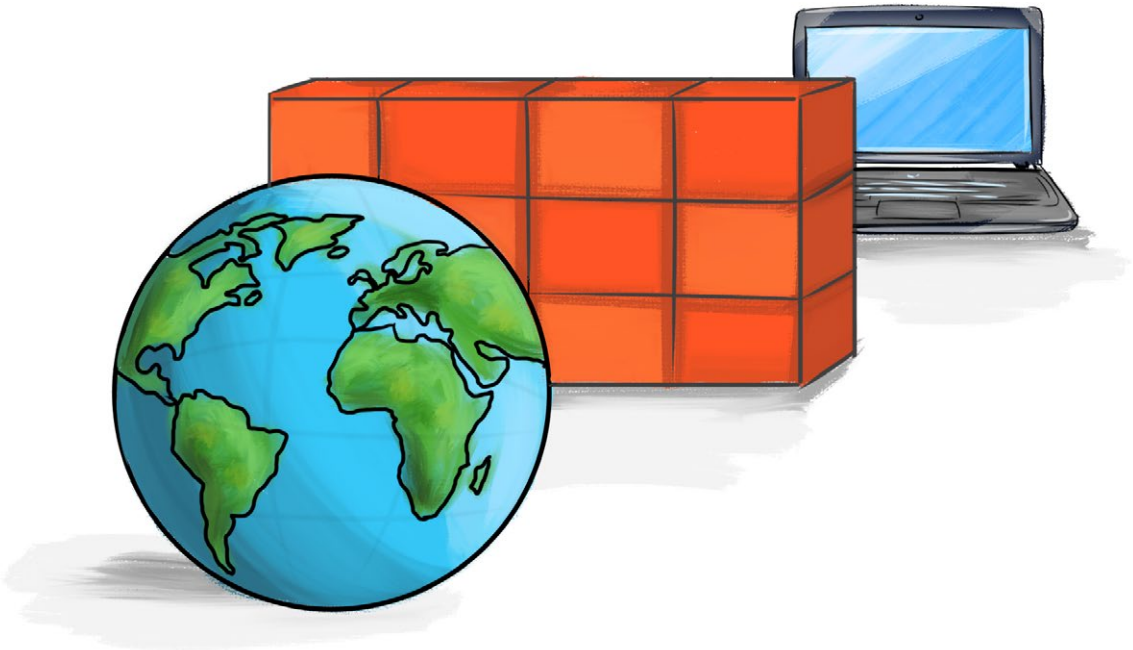


Figure 10: Firewalls

A network security system that protects a computer from unwanted connections to or from local networks and the Internet, especially Intranets. Firewalls can be implemented as both hardware and software, or a combination of both. A firewall[41] might have rules that forbid outgoing email, or connections to certain websites. Firewalls can be used as a first line of defense to protect a device from unexpected interference. They can also be used to prevent users from accessing the Internet in certain ways.

a. Hardware and Software Firewalls

Firewalls can be either hardware or software but the ideal configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins. Hardware firewalls can be purchased as a stand-alone product but are typically found in broadband routers, and should be considered an important part of your system security and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, a business networking firewall solution is available. Software firewalls are installed on your computer, like any software program, and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access to your computer. Firewalls may also be a component of your computer's operating system. For example, Windows Firewall is a Microsoft Windows application that notifies users of any suspicious activity. The app can detect and block viruses, worms, and hackers from harmful activity.

41 https://ssd.eff.org/en/glossary/firewall

a. Firewall Filtering Techniques

Firewalls are used to protect both home and corporate networks. A typical firewall program or hardware device filters all information coming through the Internet to your network or computer system. There are several types of firewall techniques that will prevent potentially harmful information from getting through:

- **Packet Filter:** Looks at each packet[42] entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.[43]
- **Application Gateway:** Applies security mechanisms to specific applications, such as FTP[44] and Telnet[45] servers. This is very effective, but can impose a performance degradation.
- **Circuit-level Gateway:** Applies security mechanisms when a TCP[46] or UDP[47] connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Proxy Server:** Intercepts all messages entering and leaving the network. The proxy server[48] effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

2.7 Encryption

Encryption involves scrambling information or a message mathematically (encrypt), so that it seems meaningless, but can still be restored to its original form by a person or device that possesses a piece of data that can unscramble it (a decryption key). This limits who can access the information or message because without the right key, it is nearly impossible to reverse the encryption and recover the original information. Encryption is one of several technologies that make up the field called cryptography.

End-to-end encryption ensures that a message is turned into a secret message by its original sender, and decoded only by its final recipient. Other forms of encryption may depend on encryption performed by third-parties. That means that those parties have to be trusted with the original text. End-to-end encryption is generally regarded as safer, because it reduces the number of parties who might be able to interfere or break the encryption.

42 https://www.webopedia.com/TERM/P/packet.html
43 https://www.webopedia.com/TERM/I/IP_spoofing.html
44 https://www.webopedia.com/TERM/F/ftp.html
45 https://www.webopedia.com/TERM/T/Telnet.html
46 https://www.webopedia.com/TERM/T/Telnet.html
47 https://www.webopedia.com/TERM/U/User_Datagram_Protocol.html
48 https://www.w ebopedia.com/TERM/P/proxy_server.html

2.8 Virtual Private Networks (VPNs)

A virtual private network (or VPN)is a method for connecting a computer securely to the network of an organization on the other side of the Internet. When connected to a VPN, all web browsing data appears to originate from the VPN itself, rather than one's own Internet Service Provider (or ISP).[49] Sensitive information could include submissions from contact forms or credit card information. Using a VPN masks the IP address[50] assigned by your ISP from the sites that you access, adding a layer of privacy. Along with masking your origin IP address, it also encrypts your data while in transit to the site you are accessing.

a. Commercial VPNs

A commercial Virtual Private Network is a private service that offers to securely relay your Internet communications via their own network. The advantage of this is that all of the data you send and receive is hidden from local networks, so it is safer from nearby criminals, untrusted local ISPs, or anyone else spying on your local network. A VPN may be hosted in a foreign country, which is useful both for protecting communications from a local government, and bypassing national censorship. The downside is that the traffic is decrypted at the commercial VPN's[51] end. That means you need to trust the commercial VPN (and the country where it is located) not to spy on your traffic. While a commercial VPN may offer "safety", it does not necessarily guarantee security.

b. Free VPNs

A free VPN is a service that gives you access to a VPN server network, along with the necessary software, without you having to pay for anything. While a free VPN may "save" you money, it may however pose a serious security risk of you losing control of your data. Examples of VPNs include; NordVPN,[52] Private Internet Access VPN,[53] Windscribe VPN,[54] CyberGhost VPN,[55] TunnelBear[56] etc.

Note! Before choosing a VPN service, always read user reviews to find out what concerns its users had. Also, always investigate the VPN service provider's reputation, and see where it is located – you probably may want to skip any service provider hosted in a country with a dubious security history.

49 https://en.wikipedia.org/wiki/Internet_service_provider
50 https://ssd.eff.org/en/glossary/ip-address
51 https://ssd.eff.org/en/glossary/commercial-vpn
52 https://nordvpn.com/
53 https://www.privateinternetaccess.com/pages/techradar
54 https://windscribe.com/upgrade?promo=WS50OFF&afftag=tomsguide-6233319505430609000&affid=fghzq9e1
55 https://www.cyberghostvpn.com/en_US/?media_source=inhouse_affiliates&lp=pro_homepage&transaction_id=1 020f5087b76582644982b711aa6e1&affiliate=futurenet%2FTechRadar&offer_id=135&coupon=YT2M&conversionpoint=externalCP&channel=External+LPs&affiliate_google_cli
56 https://www.tunnelbear.com

2.9 Tor Browser

Tor is free and open-source software for enabling anonymous communication. The name is derived from the acronym for the original software project name “The Onion Router”. Tor has inbuilt features that safeguard you from web tracking, surveillance, and fingerprinting.

2.10 DuckDuckGo

DuckDuckGo is an internet search engine that emphasizes protecting searchers’ privacy and avoiding the filter bubble of personalized search results. DuckDuckGo distinguishes itself from other search engines by not profiling its users and by showing all users the same search results for a given search term.

2.11 Work from Home Cyber Safety Tips

The novel CoronaVirus disease (COVID-19) pandemic has forced the world into social distancing as one of the main measures to contain the spread of COVID-19 and “flatten the curve”. This has forced many organizations to instruct their employees to work from home (telecommute). Telecommuting (working from home) – for whatever reason, comes with its own challenges with regards to Cyber security threats. Below is a compiled list of remote working safety guidelines.

Tips for Remote Workers

Only use Wi-Fi you trust. With an insecure connection, people in the near vicinity can snoop your traffic.

- Use Company sanctioned devices.
- Update antivirus software.
- Update all software and the operating system.
- Remember to back up periodically. All-important files should be backed up regularly. In a worst case scenario, staff could fall foul of ransomware for instance. Then all is lost without a backup.
- Make sure you are using a secure connection to your work environment. This means using a VPN or some other secure means like Teamviewer.
- Beware of phishing emails. One should be suspicious of any e-mails asking to check or renew your credentials even if it seems to come from a trusted source. Please try to verify the authenticity of any significant or suspicious request through other means, do not click on suspicious links or open any suspicious attachments.

Tips for Employers

- Focus on securing systems that enable remote access, such as VPNs. Ensure these systems are fully patched, firewalls are properly configured, and anti-malware and intrusion prevention software is installed.
- Never directly expose Remote Desktop Protocol (RDP) to the Internet (require VPN connection first).
- Implement multi-factor authentication wherever possible.
- Consider restricting access to sensitive systems where applicable Send out phishing awareness emails to your employees
- The use of unauthorized software for official purposes (known as shadow IT) can increase when working remotely, raising security and privacy risks. Ensure staff are aware of the policy, privacy and legal obligations that apply to your organization's information.
- Examine your incident response plans and, if necessary, update these to account for staff working remotely.
- Review your business continuity and contingency plans. Ensure these are up-to-date.

2.12 Video Conferencing Tools

2020 saw a major paradigm shift in in-situ traditional meetings, with the Zoom platform experiencing a boom among many. This development also witnessed a reported surge in "Zoom bombing", where meetings were intruded into by malicious individuals, and causing disruption to conference calls. To avert incidences like this, the tips below highlight measures that can be adopted.

Tips for Video Conferencing and Chat Groups

- Ensure participants can join via invitation only.
- Require a password to join the meeting
- Where possible, require administrator approval before someone can join the meeting
- Do not post meeting links to social media.
- Ensure video conferencing and chat software is always up to date.

Other Video Conferencing Tools:

- Jitsi – https://jitsi.org/
- Google Meets – https://apps.google.com/meet/
- BlueJeans – https://www.bluejeans.com
- Signal – https://www.signal.org
- Cisco Webex – https://www.webex.com
- Microsoft Teams – https://teams.microsoft.com

2.13 Digital Safety Threats: Malware & Ransomware

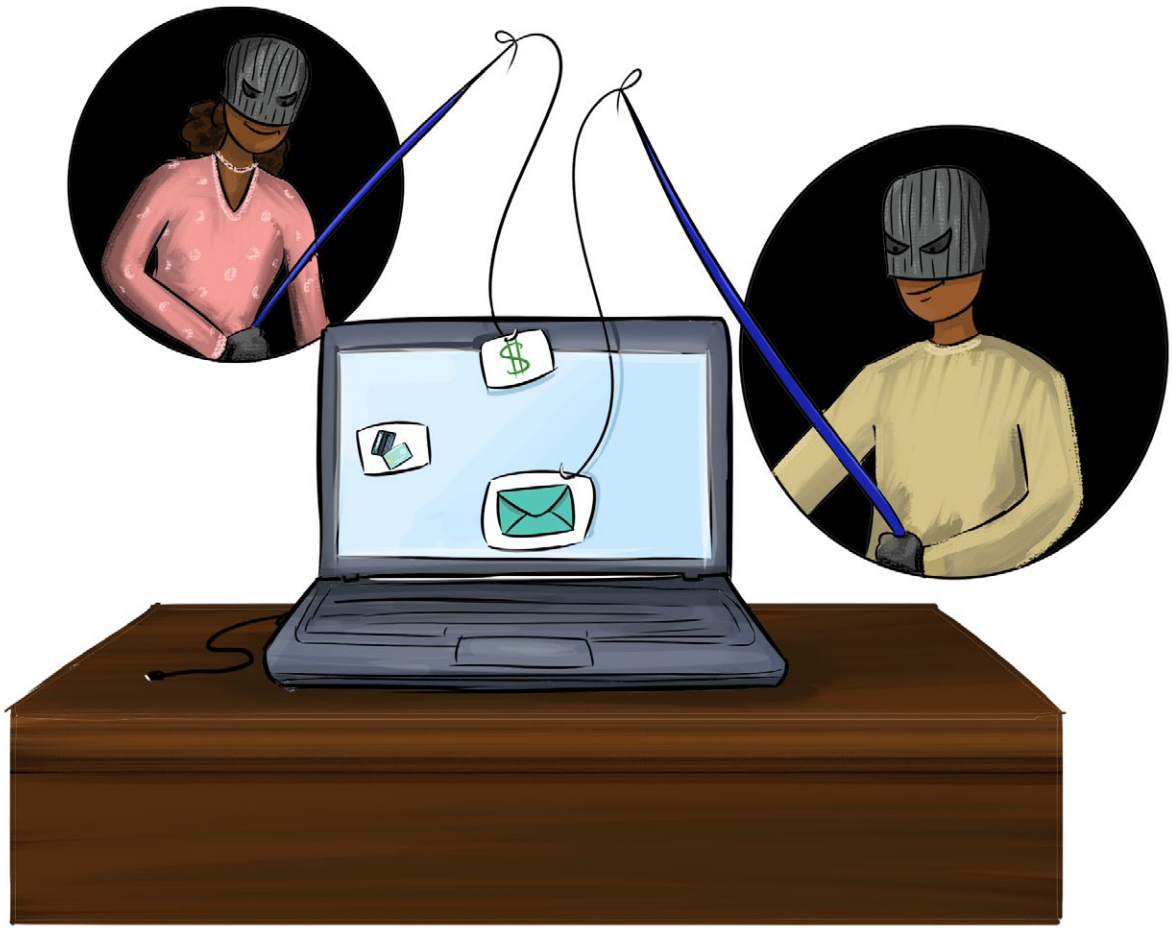


Figure 11: Spotting spam, phishing, malware and viruses

a. Malware

Malware is short for “malicious software.” It is a program or file designed to be disruptive, invasive and harmful to a computer system. Types of malware include viruses, spyware, adware and worms. It is most frequently transmitted through e-mail attachments, Instant Messages (IM), peer-to-peer downloads, phishing and misleading websites. Virus outbreaks cause harm by destroying data on infected computers and/or by increasing network traffic by triggering e-mail messages that carry the virus to all email addresses in an address book or a random combination of addresses. If viruses are not halted quickly, the flood of emails can swamp servers, disrupting email service for all. Virus software is identifiable by its actions and many tools are in place to combat the threat to the computer.

Malware Preventive Measures

With a little bit of effort, you can protect your computer and help avert more wide-ranging

problems. The following steps will prevent an attack or deal with viruses if a computer becomes infected.

- Install an antivirus[57] software on your computer.
- Keep your virus definitions up-to-date[58] even if there's no report of a new virus.
- Don't open or execute unexpected attachment.[59]
- Turn off the preview feature in your programs for added protection.
- Also turn off any program features that may automatically open an email, Instant Message, attachment file or download.

b. Ransomware

Ransomware is a type of malware that is designed to block access to all or part of a computer system until a sum of money is paid. Because attackers are looking to maximize their payday, the targets are typically larger entities (organisations, departments, colleges, businesses) that not only are likely to have the funds, but also experience a significant loss when they cannot access their systems. However, individuals are still a target of ransomware because they can be a doorway into an organization's systems. When it comes to preventing or detecting ransomware, there is no silver bullet. However, you can use some of the following techniques to help prevent and detect ransomware, which may help minimize your risk of getting malware.

Ransomware Preventive Measures

- **Limit access network file shares:**
  Only allow the level of access required by the user's business function. Limiting access to network file shares will prevent a computer infected with ransomware from spreading it to other computers on the network.
- **Keep things updates:**
  Ensure all applications are up to date. Outdated applications that don't have the most recent security patches makes them vulnerable to ransomware and other malware.
- **Use Anti-virus:**
  An antivirus is a tool that helps to detect and remove malware from your computer. You should always keep an updated antivirus to enable you to detect and clean ransomware that may have been installed on your computer.

57 https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/anti-virus
58 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/updates-patching
59 https://cybersecurity.osu.edu/cybersecurity-you/avoid-threats/phishing

2.14 Surveillance and mass surveillance

It includes location tracking, deep packet inspection, facial recognition, mass monitoring and the interception of communications. Surveillance has a detrimental effect on writers' and reporters' willingness to research and publish stories, and makes it harder for them to protect sources.

2.15 Phishing attacks

"Phishing" or "spear phishing" campaigns often use links or attachments in e-mail or on social media that carry malware. Once these links are clicked on, they can do significant damage. Malware can allow attackers to get any information they want from a compromised computer, including a journalist's personal information, data and sources.

2.16 Fake domain attacks

These are websites created to impersonate legitimate ones for malicious purposes. Independent media and civil society websites have often been victims. The fake sites serve up malware or publish false information in an effort to discredit the real media site or a particular journalist.

2.17 Man-in-the-Middle (MitM) attacks

Attackers insert themselves between a user and a target site. For example, a wireless router is configured to act as a Wi-Fi hotspot in a public place, to trick people into thinking it's legitimate. When individuals connect to it, the attacker has instant access to the data passing through the router.

2.18 Denial of Service (DoS) attacks

These attacks are quite common, and involve one or more computers and Internet connections flooding a server with traffic, making it inaccessible to others. For journalists, these attacks prevent information from reaching the public and can become costly, as visitor numbers drop and technical help is needed.

2.19 Cyberstalking

Cyberstalking refers to the use of the Internet or other electronic means to stalk and or harass an individual, group, or organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, or gathering information that may be used to threaten, embarrass or harass.

2.20 Cyber bullying

Cyber bullying is the use of electronic means such as e-mail, social media, instant messaging, and other forms of online communication with the intent to abuse, intimidate, or overpower an individual or group.

Resources

1. https://tinyurl.com/y2kkmckg
2. https://tinyurl.com/y37nrxd7
3. https://tinyurl.com/yyu2y5ub
4. https://tinyurl.com/yxzfprhj
5. https://tinyurl.com/y25p5q3e
6. https://tinyurl.com/y3szuuhz
7. https://tinyurl.com/y692p5yw
8. https://tinyurl.com/yy92uvrc
9. https://tinyurl.com/y28vrj7z
10. https://tinyurl.com/yxpd2vpg

Chapter III

3.1 Digital and Physical Security

a. Digital Security at Protests

At some point in their line of work, digital rights actors find themselves involved in protests in the quest to have their voices heard. Carrying digital devices to these protests can however be used against protestors, considering law enforcement groups have digital surveillance tools, such as fake cell phone towers and facial recognition technology, that could be used to identify protestors and monitor their movements and communications, thus jeopardizing their security and privacy. Before heading to peaceful demonstrations, protesters should consider taking into account their digital privacy. Below are some things they should bear in mind.

b. Keeping protest prep private

Having a trustworthy Virtual Private Network service could help protest organizers disguise their Internet traffic. Alternatively, protestors can make use of tools such as Tor browser,[60] which mask a user's online activity by blocking trackers and encrypting their network traffic multiple times. Also very vital, is ensuring protest-related organizing is conducted over end-to-end encrypted Apps rather than plain text messages (otherwise known as SMS)

c. Full Disc Encryption of digital devices

In the event that your device is confiscated by law enforcement officers, and or is lost or stolen, full-disk encryption can ultimately help protect the data stored on your device. Android[61] and iOS[62] devices have inbuilt full-disk encryption capabilities. These should be protected using strong passwords to avoid being breached using a brute-force attack.

d. Install Signal

Signal is an app available on both iOS[63] and Android[64] that offers strong end-to-end encryption to protect both text messages and voice calls. In addition to encrypting one-to-one communication, Signal enables encrypted group chats. The app also recently added the functionality of having messages disappear anywhere from 10 seconds to a week after they are first read. In contrast to some other services like SnapChat, these ephemeral messages will never be stored on any server, and are removed from your device after disappearing.

60 https://www.torproject.org/
61 https://source.android.com/security/encryption/full-disk.html
62 https://www.apple.com/business/docs/iOS_Security_Guide.pdf
63 https://ssd.eff.org/en/module/how-use-signal-ios
64 https://ssd.eff.org/en/module/how-use-signal-android

e. Backup your data

Take precautions to limit the potential costs of losing access to your device, whether it is lost, stolen or confiscated by law enforcement. Back up your data regularly and store that backup in a safe place to save yourself from a headache later on.

f. Burner phone

For protestors that are worried about having their phone tracked, a temporary but ideal solution would be getting a “burner” phone, a prepaid device paid for in cash and used for the express purpose of staying in touch with people during a peaceful protest. Burner phones can give users the benefit of being able to stay in touch with people – especially if things get dicey – without exposing all the data on their everyday device. Alternatively, putting your phone in airplane mode could serve the same purpose. Further reading available at https://ssd.eff.org/en/module/attending-protest.

g. Physical Security

Physical threat to digital rights activists is as real as digital security threats. These threats range from arrests, harassment, confiscation of devices, and detention by state actors. This puts them at a potentially high risk, a factor that jeopardizes their security. In order to mitigate physical security threats, digital rights activists are urged to be alert to signs of threat to their personal security, taking into consideration their environment, the laws and the type of people in the community. The rule of the thumb is - in order for a digital rights actor to succeed in protecting others, their own security must be guaranteed.

3.2 Mitigating Physical Security Threats

To mitigate risk, digital rights actors are encouraged to take the following into consideration:

a. Accepting the risk:

Accepting the risk means that the victim who is in need of protection should be able to know that he or she can be at risk while executing his or her activities. With such awareness, the person is expected to be prepared to mitigate the risk or potential of risk. For example, when you are going out for humanitarian work in a war zone, you need to know that your security is at stake; therefore you need to be prepared to run when necessary, to call for help and you need to contact and explain your mission to the combatants involved in the fighting so that they can grant you access into the area. Also, when you know that your data can be at risk of cyber-attack, you need to create a strong password, do fact checking of the digital platforms you intend to use, share your data to trusted persons and also store your data in different storage devices.

b. Avoiding the risk:

Knowing the risk is one thing and avoiding it is another. When you learn of a risk, you need to avoid it by all means; you do not need to claim rights or power at that time. To avoid risk, your communication and actions should reflect and or change according to the situation you find yourself in. That is you need to check your body language and use your words wisely, you need to evaluate the environment before you start any activities or engage with people, you need to understand whether there is a potential risk or not, and finally when it proves that you are a target, you need to respond fiercely to resist your attacker.

c. You should have and present your ideology to the right people:

Your ideology may pose you at risk when you publicize it. As a human rights advocate, you need to have a level of knowledge on whom you entrust with your information or associate with because people are not obliged to accept your ideas.

d. As a representative of an organization you need to know more about yourself and the organization:

To avoid risk as a leader, you need to know who you are, what you do and the people you represent. It is very important for you to know everywhere you go; such preparedness becomes very handy in cases where you become under custody as a suspect. The way you present yourself, position and organization has a significant influence on how you will be treated by your custodians. In most cases, the innocent suspect will be released after properly presenting him/herself. Body language, choice of words and total composure needs to be well managed while under arrest and investigation.

e. Context:

Be it within your area, out of your area or anywhere within the globe, you need to take into consideration and answer the following questions; 'Who am I? Where am I? Who are they'? These questions are very important because whatever activities you are carrying out needs to take the above questions into consideration for your security. For example, a human rights advocate cannot be within the army barracks and condemn the atrocities committed by the soldiers; this reveals the failure to crosscheck by answering the questions above and not taking into context the security measures within the scope of your profession and external factors. The tendency in such a case is that you will be arrested and detained for expressing your opinion to their hearing and at their premise.

f. Avoid risk zones:

Areas like borders of towns, crowds, banks, traffic areas, public gatherings, conflict or war areas etc. are risk zones and we need to learn when and what time to visit the areas, taking into consideration your profession and position. For example a human rights activist is not advised to visit conflict zones without the guarantee of safety from the belligerents.

Case study is the Anglophone Regions of Cameroon where there is conflict between the separatists and government forces; humanitarian workers for their security cannot access confrontation zones without safe passage assurance from the combatants. This is because they may be hurt by stray bullets, arrested or kidnapped if they fail to have security assurance from the combatants.

g. Dressing:

you need to be conscious of your appearance and understand how to dress when carrying out humanitarian activities. For example, if you are a humanitarian worker, when going out for field work you need to wear light shoes and dress in such a way that you can easily escape a scene or run when there is a need. If your area is not secured, avoid wearing or dressing expensively in such areas because you may be targeted based on how they have observed that you dress. Avoid contacting people you do not know in isolated areas because they may be threats to your security and avoid wearing tight-fitting clothes because it may deter you from running when the need arises.

h. Do not resist at gunpoint or in the army barracks:

When you are arrested or kidnapped or surrounded by thieves, do whatever they want you to do in order to protect your life. Do not resist because they can kill you; consider your security first.

i. Have your basic needs whenever you are out for a mission including medical first aid box:

Whenever you are out on a mission, as a leader/actor, you should take alongside your basic needs in reasonable quantities taking into consideration your health, your journey, the climatic conditions of the place, financial conditions, your instincts etc. These will be for your physical security because you must accept the risk and predict possible solutions before going out for missions.

j. Always have trusted and networking contact:

In every profession especially when it comes to risky jobs like human rights activism, you need to predict the risk of arrest, kidnapping and or the attack on your data. As mitigating factors, you need to have trusted persons whom you can share your information to, including the location you are going to, at which time you are expected to be there, at which time you are expected to be back, what is expected to be done in case there is a call for concern, etc.

k. Keep, know and memorize emergency contacts:

You need to have emergency contact numbers such as, the police, ambulance service, fire service, hospital, etc. Download and install applications that can track your device when you

are in trouble. Further reading: https://tinyurl.com/y5wje4zk

Resources

11. https://tinyurl.com/y34p99o6
12. https://tinyurl.com/yy4t25hm
13. https://tinyurl.com/y2nn2ot9
14. https://tinyurl.com/y32w6ra
15. https://tinyurl.com/y369rudo
16. https://tinyurl.com/y6arpfw6
17. https://tinyurl.com/y85p49a3
18. https://tinyurl.com/y33cxu2u
19. https://tinyurl.com/y5wje4zk
20. https://tinyurl.com/y6spa5zk
21. https://tinyurl.com/y4tv7srz

Chapter IV

4.1 Internet Shutdowns

Figure 12: Internet Shutdown

Article 19 of the Universal Declaration of Human Rights guarantees everyone the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. However, in recent years, there has been an increased tendency of African states resorting to information controls over their citizens. This has turned the Internet into a more volatile space, and incidences of challenges posed to activists, human rights defenders, dissidents, and journalists are reportedly on the rise.

Authoritarian regimes have resorted to using digital tools and tactics such as Internet

shutdowns, online censorship, and digital surveillance to clamp down on free expression. According to Freedom House's Freedom on the Net 2018, "governments around the world are tightening control over citizens' data and using claims of 'fake news' to suppress dissent, eroding trust in the internet as well as the foundations of democracy." A 2018 CIPESA Report[65] revealed that up to 22 African governments had ordered network disruptions in the last four years and since the start of 2019, 6 African countries – Algeria, the Democratic Republic of Congo (DR Congo), Chad, Gabon, Sudan and Zimbabwe – had experienced internet shutdowns.

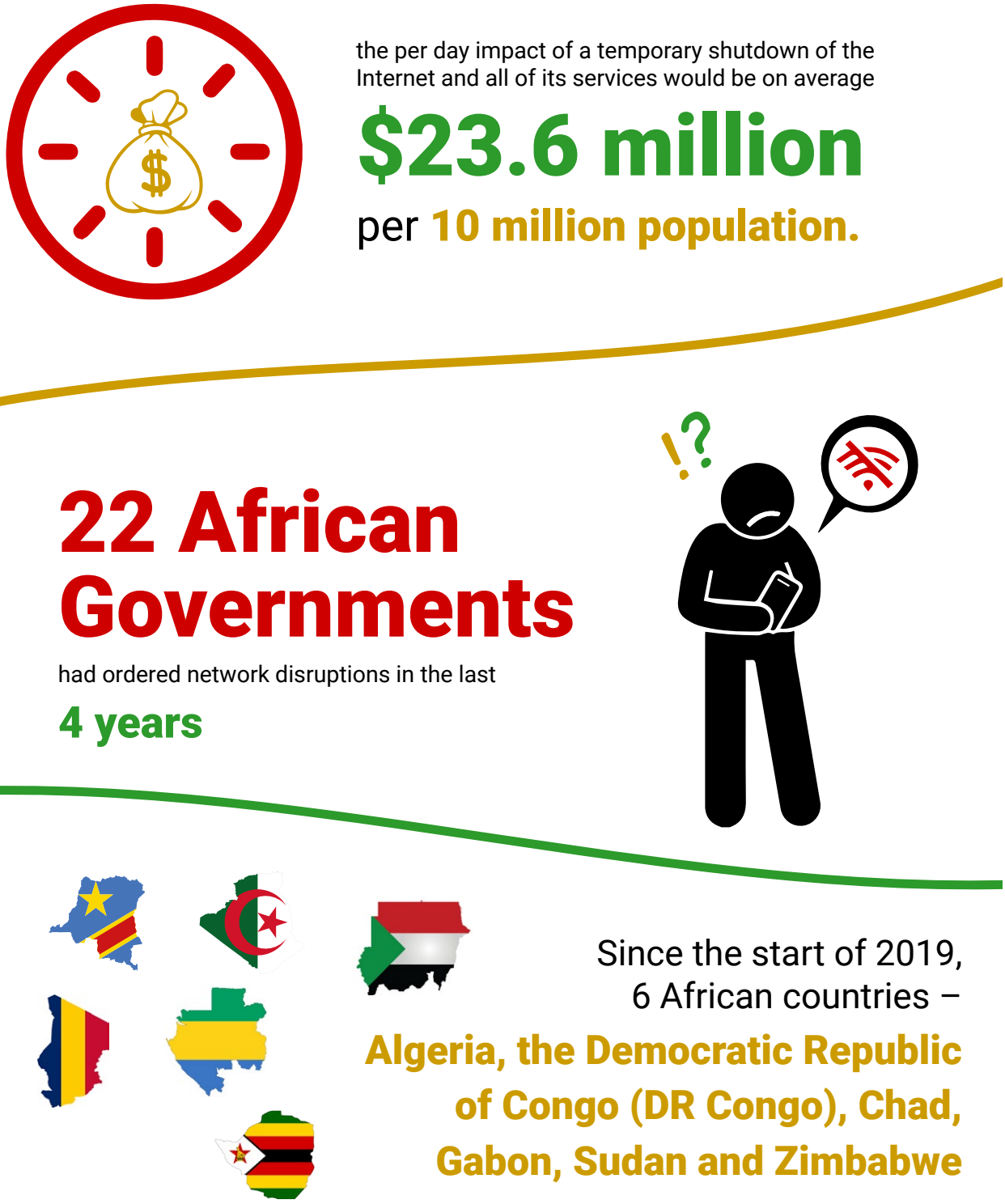


Figure 13: Internet shutdown data in Africa

65 https://cipesa.org/2019/03/despots-and-disruptions-five-dimensions-of-internet-shutdowns-in-africa/

Further, a Paradigm Initiative 2019 report[66] revealed that a number of African governments have been shutting down the Internet for political reasons, passing stringent regulations on online content, and or employing the use of targeted spyware attacks against human rights defenders. The report added that this export of Chinese and Russian models of so-called "rule of law" tactics towards control of the Internet has seen tightening government control and digital rights violations through legislation that is ostensibly written to promote law and order in African societies. The shutdowns have had adverse economic impacts in the countries in question. A Deloitte study[67] reveals that for a highly Internet connected country, the per day impact of a temporary shutdown of the Internet and all of its services would be on average $23.6 million per 10 million population. Despite this move by various states to clamp down on digital spaces, and in the process limiting the work of those on the frontlines of human/digital rights advocacy, a number of Internet anonymity and circumvention tools such as VPNs, and Web based proxies offer hope to human rights actors, digital rights defenders, journalists, whistle blowers amongst others.

4.2 Circumventing Internet Shutdowns and Censorship

Internet anonymity and circumvention tools such as VPNs, Tor Browsers, and Web based proxies do offer hope to human rights actors, digital rights defenders, journalists, whistle blowers amongst others.

a. Virtual Private Network (VPN)

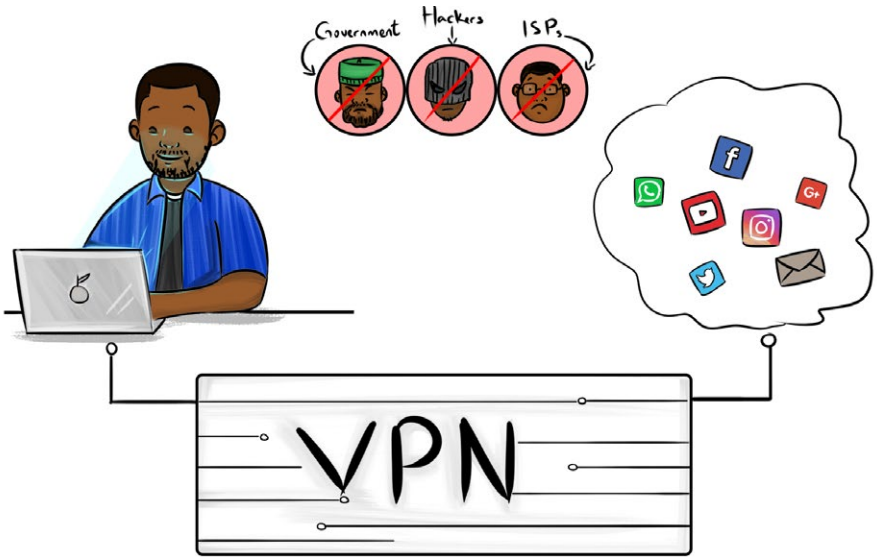


Figure 14: Using VPNs

66 http://paradigmhq.org/download/dra19/
67 https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the- economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html

As already discussed in chapter II under digital safety, a virtual private network (VPN) is a method for connecting your PC and or Internet connected device securely to the network of an organization on the other side of the Internet. When you use a VPN, all of your Internet communications are packaged together, encrypted, and then relayed to this other organization, where they are decrypted, unpacked, and then sent on to their destination. To the organization's network, or any other computer on the wider Internet, it looks like your computer's request is coming from inside the organization, not from your location. VPNs are used by individuals to bypass local censorship, or defeat local surveillance.

4.3 Measuring Internet Shutdowns and Censorship

a. The Open Observatory of Network Interference (OONI)

The Open Observatory of Network Interference (OONI) is a free software project that aims to empower decentralized efforts in increasing transparency of Internet censorship around the world. OONI develops free and open source software[68] called **OONI Probe** that you can run to measure:

- Blocking of websites;
- Blocking of instant messaging apps (WhatsApp, Facebook Messenger and Telegram);
- Blocking of censorship circumvention tools (such as Tor and Psiphon);
- Presence of systems (middleboxes) in your network that might be responsible for censorship and/or surveillance; and
- Speed and performance of your network.

By running OONI Probe,[69] you can collect data that can potentially serve as evidence of Internet censorship since it shows how, when, where, and by whom it is implemented.

4.4 Advocacy against Internet Shutdowns in Africa

a. The Cost of Shutdown Tool (COST)

COST is a data driven online tool for measuring the cost of Internet shutdowns, and convincing governments to keep the Internet on. The tool enables anyone – including journalists, researchers, advocates, policy makers, businesses, and many others – to quickly and easily estimate the economic cost of Internet disruptions. Building upon methodologies devised by the Brookings Institution[70] and CIPESA[71] Cost of Shutdown Tool (COST) estimates economic cost of internet shutdowns, mobile data blackouts and social media restrictions using thousands of regional indicators from the World Bank, ITU, Eurostat and U.S. Census.

68 https://github.com/ooni/probe
69 https://ooni.org/install/
70 https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf
71 https://cipesa.org/

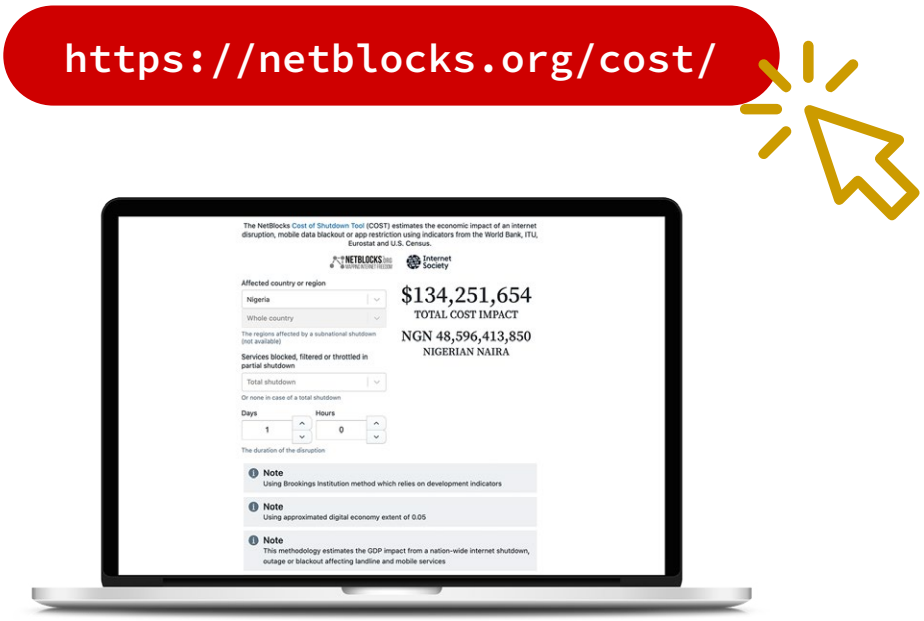


Figure 15: Advocacy against Internet Shutdowns in Africa

b. #KeepItOn Campaign

This global campaign spearheaded by AccessNow, seeks to urge governments the world over not to shut down the Internet and allow the free flow of information.

Resources

1. https://tinyurl.com/y4sul3dd
2. https://tinyurl.com/y5xxucxy
3. https://tinyurl.com/y49ckklq
4. https://tinyurl.com/y669mw6v
5. https://tinyurl.com/y6dhe2o4
6. https://tinyurl.com/y46tnwuk

Glossary

Add-on - An add-on is a piece of software that modifies other software by changing how it works or what it can do. Often add-ons can add privacy or security features to web browsers or email software. Some add-ons are malware, so be careful to install only those that are reputable and from official sources.

Anonymity - The condition of being anonymous

Anti-virus - Anti-virus software is software for your PC used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses. Some examples of anti-virus software are McAfee, Avast, AVG, and Kaspersky.

Censorship - Internet censorship is the control or suppression of what can be accessed, published, or viewed on the Internet enacted by regulators, and or governments.

Circumvention - The use of various methods and tools to bypass Internet censorship.

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

Digital Hygiene - Refers to organizing the files on your PC, to locking down your social media accounts, to introducing new apps or technologies to make your digital life easier or more secure. Digital Rights - Digital rights are basically human rights in the Internet era. Encryption - A process that takes a message and makes it unreadable except to a person who knows how to “decrypt” it back into a readable form.

Encryption Key - An encryption key is a piece of information that is used to convert a message into an unreadable form. In some cases, you need the same encryption key to decode the message. In others, the encryption key and decryption key are different.

Firewall - A tool that protects a computer from unwanted connections to or from local networks and the Internet. A Firewall might have rules that forbid outgoing email, or connections to certain websites. Firewalls can be used as a first line of defense to protect a device from unexpected interference. They can also be used to prevent users from accessing the Internet in certain ways. Internet shutdown – An Internet shutdown is an intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information

IP Address - An IP (Internet Protocol) address is what uniquely identifies connected devices on the Internet.

Malware - Malware is short for malicious software: programs that are designed to conduct unwanted actions on your device. Computer viruses are malware. So are programs that steal passwords, secretly record you, or delete your data.

Operating System (OS) - A program that runs all the other programs on a computer or device. Windows, Linux, Android and Apple's OS X and iOS are all examples of operating systems.

Password Manager - A password manager is a tool that creates and stores passwords for you, so you can use many different passwords on different sites and services without having to memorize them.

Passphrase - A passphrase is a kind of password, only that it's longer that a password which is usually a single word.

PC (Personal Computer) - A multi-purpose computer

PGP - PGP or Pretty Good Privacy was one of the first popular implementations of public key cryptography. PGP was developed by Phil Zimmermann1991 to help activists and others protect their communications.

Proxy - A proxy is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources. A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.

Security question - These are password related queries to which only you are supposed to know the answer.

Software - It's a generic term used to refer to applications, scripts and programs that run on a device

Tor - Tor is free and open-source software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".

Two Factor Authentication (2FA) - Two-factor authentication (or "2FA") is a way to let a user identify him or herself to a service provider by requiring a combination of two different authentication methods. These may be something that the user knows (like a password

or PIN), something that the user possesses (like a hardware token or mobile phone), or something that is attached to or inseparable from the user (like their fingerprints).

URL (Uniform Resource Locator) - The address of a World Wide Web page.

Virtual Private Network (VPN) - A Virtual Private Network is a network we can access to connect to the Internet via an encrypted tunnel. Our ISP, or anyone sniffing on the free Wi-Fi we're using to access the web, can only see our connection to the VPN service, while the website we are visiting will only record a connection from the VPN servers. To decide which is the best VPN for you, read this guide.

Virus - A PC virus is a piece of code with the capability of copying itself and typically has a detrimental effect, such as corrupting a computer system or destroying data.

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

AYETA

Digital Rights Toolkit

PARADIGM INITIATIVE

ParadigmHQ.org

@ParadigmHQ

/ParadigmHQ

/ParadigmHQ

Kingdom of the Netherlands

Stanford PACS
Center on Philanthropy and Civil Society
—
Digital Civil Society Lab