MODULE 1

DIGITAL RIGHTS AND RESPONSIBILITIES

PUBLICATION DETAILS PAGE

First published in March 2020

PUBLISHED BY :
MinorMatters an initiative by the National Christian Evangelical Alliance of Sri Lanka

WEB : www.minormatters.org

EDITOR: Nalaka Gunawardene

PROJECT COORDINATION BY:

Yamini Ravindran, *Director, Legal and Advocacy*
Shalomi Daniel, *Legal and Advocacy Coordinator, Religious Liberty & Social Justice Commission*
Akshina Palihawadana, *Media Strategy Officer, Religious Liberty & Social Justice Commission*

COVER DESIGN: Sanjayan Ariadurai

PAGE LAYOUT AND DESIGN: Shenal Jesudian

DISCLAIMER:

The analysis and opinions expressed in this publication are those of the contributors and editors. They are not necessarily those of the National Christian Evangelical Alliance of Sri Lanka, and do not commit the organisation.

DIGITAL RIGHTS AND RESPONSIBILITIES

As we increasingly conduct our lives online – for studying, working, socializing, community mobilizing, shopping and other purposes – our digital rights are becoming more important.
Everyone has the right and freedom to use different types of digital technology and services of their choice, but such use of technology should be done in a responsible and ethical manner.

Digital technologies are a double-edged tool. That means they can be used to do good or to cause harm. Depending on who uses it with what intention, they can become means through which human rights are promoted, exercised or violated. All users of digital technologies need to understand these realities. Only through awareness and caution can we optimize the digital benefits and avoid or minimize digital pitfalls.

For example, digital tools enable the easy gathering, processing and sharing of data on a larger scale as never before. Do we know how our data is being used by governments or internet companies such as Facebook and Google? Is our data being handled fairly and carefully, or shared (even sold) without our knowledge or consent? Are governments engaging in mass electronic surveillance of our private email and other communications?

Despite various laws, regulations and technical safeguards that are in place in many countries, it is still possible for governments, companies and even cyber criminals to collect some of our data and to track our online movements and communications. We as users of digital and web services need to be better aware of our digital rights as well as how they can be violated.

Just as importantly, we need to know how we can protect our data and other digital assets by taking certain precautions. At the same time, we have to ensure that we ourselves do not violate other users' digital rights or make them vulnerable to digital risks.

In this module, we explore the concepts of digital rights and digital responsibilities. The modules that follow will introduce you to the basics of digital communications and digital security.

KEY TERMS

Digital rights can mean different things to different people - from digital (copy)rights to digital human rights.

Digital human rights, often simply referred to as digital rights, describes the human rights that allow individuals to access, use, create, and publish digital media or to access and use computers, other electronic devices or communications networks.

In the copyrights sense, Digital Rights refers to the relationship between copyrighted digital works (such as film, music and art) and user permissions and rights related to computers, networks and electronic devices. Digital rights can also mean the access to, and control of, digital information.

Digital Rights Management or DRM refers to a collection of systems used to protect the copyrights of digitally stored media. These include digital music and movies, as well as other data that is stored and transferred digitally.

In this document, by Digital Rights we mean digital human rights – and not digital copyright.

Source: http://www.ictliteracy.info/

HUMAN RIGHTS AND DIGITAL RIGHTS

All digital rights are rooted within the global framework of fundamental human rights that have evolved historically in different societies and cultures.

Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion or any other factors. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more. Every human being is entitled to these rights, without discrimination.

The most important document that captures these rights is the Universal Declaration of Human Rights (UDHR). It was drafted by representatives with different legal and cultural backgrounds from all regions of the world and was adopted by the United Nations General Assembly in Paris on 10 December 1948 as a common standard of achievements for all peoples and all nations. UDHR sets out 30 fundamental human rights to be universally protected which includes the right freedom of expression, freedom from torture, right to privacy and the right to education. It has been translated into over 500 languages.

The protection of these rights is done through a series of international human rights treaties and other legal instruments adopted since 1945 – together, these make up international human rights law. Most countries of the world (including Sri Lanka) have signed and ratified these treaties.

The United Nations Human Rights Council (UNHRC) is a United Nations body whose mission is to promote and protect human rights around the world. With its headquarters located in Geneva, Switzerland, UNHRC holds regular sessions three times a year, in March, June, and September.

In recent years, some human rights have been identified as particularly relevant in cyberspace. These include the right: to freedom of expression, the right to data protection and privacy, and freedom of association. Furthermore, the right to education and multilingualism, consumer rights, and capacity building in the context of the right to development have also been identified as digitally significant.

The ever-increasing generation of data in cyberspace and the powerful algorithms-based technologies pose serious risks to individual privacy as well as to other human rights. The trans-border nature of the internet itself presents significant challenges for existing legal and institutional frameworks.

Reconciling these new realities with the existing human rights frameworks has not been easy. Some have asked: should there be additional rights for the digital realm or cyberspace?

In June 2016, the UN Human Rights Council adopted a resolution saying that "the same rights that people have offline must also be protected online". This is a significant political commitment by UN member states (which includes Sri Lanka). Based on their existing obligations under international human rights law, governments have pledged to protect freedom of expression, privacy and other human rights online.

The resolution called upon all UN member states "to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development..."

[1] Full text at: https://www.un.org/en/universal-declaration-human-rights/index.html
[2] A non-legal overview of these can be found at: https://www.un.org/en/sections/issues-depth/human-rights/
[3] Official website of HN Human Rights Council: https://www.ohchr.org/EN/pages/home.aspx

WHAT IS AN ALGORITHM?

An algorithm is a step by step method of solving a problem or doing something. It is commonly used for data processing, calculation and other related computer and mathematical operations. An algorithm is also used to manipulate data in various ways, such as inserting a new data item, searching for a particular item, or sorting an item.

Source: https://www.techopedia.com/definition/3739/algorithm

WHAT ARE DIGITAL HUMAN RIGHTS?

Henceforth, when we refer to Digital Rights, we mean digital human rights – and not digital copyrights, which is a related but separate discussion.

The World Wide Web is the graphical interface of the internet which is what most people use. It was invented in 1989. During its first decade, during the 1990s, most users could only browse websites – creating new web content required programming skills. Users could generate their own content only in emails and chats. At that time, the main concern was how to get more people to access the web.

Access has vastly improved in both developed and developing countries. By end 2018, a little over half of the global population was online: the UN's International Telecommunications Union (ITU) estimated that 51.2% of the global population, or 3.9 billion people, were using the internet. The percentage of people using the internet in the Asia Pacific region was 47%. This means that while more people are connected today than ever before, there still remain large numbers who cannot access these services.

In the mid-2000s, after social media platforms emerged, every internet user could both consume web content and also publish their own content online if they wanted. This brought up new possibilities as well as new challenges.

The Association for Progressive Communication (APC) is an international network of organizations founded in 1990 to provide communication infrastructure, including Internet-based applications, to those working for peace building, human rights and sustainability. In 2006, they came up with an Internet Rights Charter which covered the following themes:

- Internet access for all
- Freedom of expression and association
- Access to knowledge
- Shared learning and creation – free and open source software and technology development
- Privacy, surveillance and encryption
- Governance of the internet
- Awareness, protection and realization of rights

As ICTs evolve, the digital opportunities and challenges also change. Over the years, human rights activists, researchers and civil society groups have been updating the debate around digital rights.

[4] The promotion, protection and enjoyment of human rights on the Internet. UNHRC Resolution A/HRC/^{32}/L.^{20}. Adopted on ^{27} June ^{2016}. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/^{32}/L.^{20}
[5] https://news.itu.int/itu-statistics-leaving-no-one-offline/

> "THE INTERNET IS A GLOBAL PUBLIC SPACE THAT MUST BE OPEN, AFFORDABLE AND ACCESSIBLE TO ALL. AS MORE AND MORE PEOPLE GAIN ACCESS TO THIS SPACE, MANY REMAIN EXCLUDED. LIKE THE PROCESS OF GLOBALISATION WITH WHICH IT HAS BEEN CLOSELY INTERTWINED, THE SPREAD OF INTERNET ACCESS TAKES PLACE WITH UNEVEN RESULTS AND OFTEN EXACERBATES SOCIAL AND ECONOMIC INEQUALITIES. HOWEVER, THE INTERNET AND OTHER INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTS) CAN BE A POWERFUL TOOL FOR SOCIAL MOBILISATION AND DEVELOPMENT, RESISTANCE TO INJUSTICES AND EXPRESSION OF DIFFERENCE AND CREATIVITY."

OPENING WORDS OF THE APC
INTERNET RIGHTS CHARTER, 2006

[6] APC Internet Rights Charter, 2006: https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter

GENDER DIMENSIONS OF INTERNET USE

Men and women access and use the internet differently, and their online experiences are also different.

For a start, women are less likely to be internet users in most countries regardless of their country's region or income level. For example, a countrywide survey in Sri Lanka, conducted by LIRNEasia in 2018, found that girls and women aged 15 to 65 are 34% less likely to have used the internet than men of the same age range.

Internet in India 2017 report, released by the Internet and Mobile Association of India, says women made up only 30% of internet users in India in 2017.

When women get online, they face particular types of online harassment for simply being women – in many cases, the frequency and intensity of such harassment are greater
(this is discussed in some detail in later modules).

Women’s rights activists and gender researchers have been analyzing digital rights and responsibilities from gender perspective, and through a feminist lens. They strongly advocate for a holistic approach that recognizes the blurring of the online and offline worlds. This means that the targeting and harassment of women that is widespread in society is now found in cyberspace as well. It needs a strong response in both spheres.

The Feminist Principles of the Internet (FPI) have emerged as a set of statements that provide a framework for women's movements to articulate and explore issues related to technology. These offer a gender and sexual rights lens on critical internet-related rights. First drafted in April 2014, their most recent updated version was published in 2016. The process was facilitated by the Association for Progressive Communications (APC), a global network of civil society groups.

Currently there are 17 principles total, which are organized in five clusters: Access, Movements, Economy, Expression, and Embodiment.

The preamble reads: “A feminist internet works towards empowering more women and queer persons – in all our diversities – to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy. This integrates our different realities, contexts and specificities – including age, disabilities, sexualities, gender identities and expressions, socioeconomic locations, political and religious beliefs, ethnic origins, and racial markers.”

A key point in these principles is that issues online are closely linked to what is ‘offline’, or what happens in the physical world. There is also a strong overlap between online and offline that needs to be studied when advocating digital rights for everyone.

The Feminist Principles of the Internet make us raise key questions like these:

- Who has access to the digital realm?
- Of those who have access, are they able to express themselves freely?
- What are the repercussions for doing so – especially for the already vulnerable groups?
- Who creates and shares content, and how inclusive is this content?
- What are the consequences and opportunities available in the digital world, and what do we need to do to ensure that everyone has equal access to the opportunities?

[7] https://lirneasia.net/2019/05/afteraccess-findings-from-sri-lanka-released-in-colombo-today-event-report/
[8] Read all Feminist Principles of the Internet at: https://feministinternet.org/en

> “WOMEN HAVE CONSISTENTLY BEEN DENIED ACCESS TO PUBLIC SPACES BECAUSE MEN CANNOT CONTROL THEIR ‘MASCULINITY’ IN PUBLIC. AS THE USE OF TECHNOLOGY ROSE, WOMEN WERE ALSO BARRED FROM USING THE INTERNET, BECAUSE MEN ALREADY OCCUPIED THE VIRTUAL SPACES BEFORE WOMEN HAD ACCESS TO IT. ONE REASON WHY WOMEN ARE CONSTANTLY THE SUBJECT OF ONLINE ABUSE IS PRECISELY BECAUSE THEY ARE A MINORITY ON THE INTERNET.”

NIGHAT DAD, LAWYER, HUMAN RIGHTS ACTIVIST
AND EXECUTIVE DIRECTOR OF THE DIGITAL RIGHTS
FOUNDATION IN PAKISTAN

FREEDOM OF EXPRESSION ONLINE

Article 19 of the UDHR covers the right to freedom of opinion and expression - which includes guaranteeing the right to speak, publish and broadcast freely, and the right to receive such information, regardless of borders. This is one of the most important and prominent rights in the digital age.

“The open flow of information has been key to the Internet’s transformative effect in modern society. In order to safeguard its benefits, the right to free expression must be defended when addressing issues of content and defining the technical management of the Internet’s architecture.”
Article ^{13} (advocacy organization)
https://www.article^{19}.org/issue/digital-rights/

The internet has become an important global platform for private communications, self-expression, information sharing as well as publishing and broadcasting. It has also emerged as a vital space where democracy and human rights activists can mobilize and advocate for political, social and economic reforms.

At the same time, the digital technologies that make this possible can also be used to limit access to information through content blocking and full-scale internet shutdowns, or stifle expression through state surveillance on a massive scale that was previously not possible. So it is important for us to understand both the opportunities and threats.

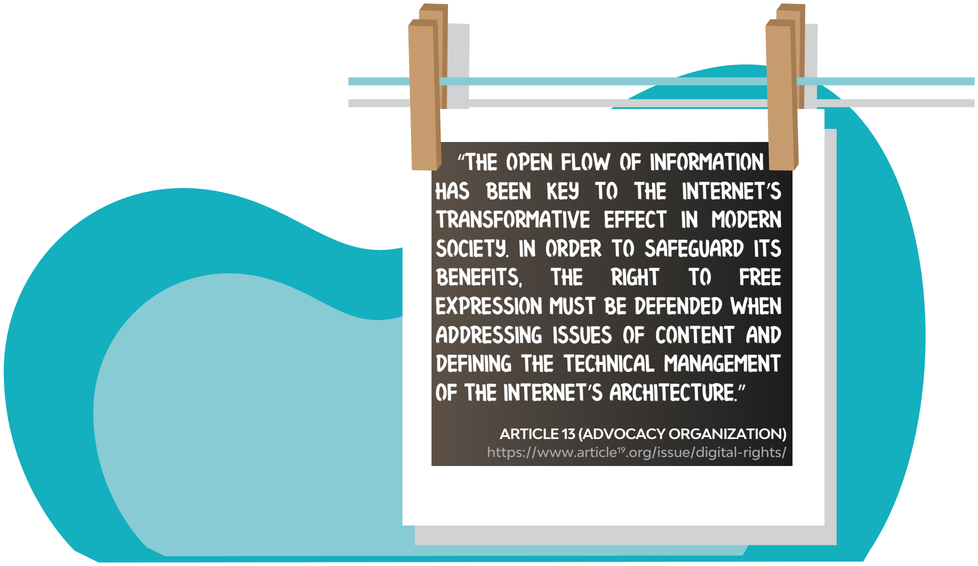
Today, the web in general and social media in particular enable anyone, anywhere with internet access and basic digital skills to express themselves to a potential global audience. It can be through blogs, posts or comments on social networks like Facebook and Twitter, or image-driven expressions on platforms like Instagram and YouTube. There are dozens of other platforms, most of them allowing free membership and are easy to use (i.e. without having any coding skills).

Until recently, this ability to publish was limited to mass media companies like newspapers, radio and television – setting up and operating these require high investments and trained professionals like journalists and editors. The web has made it cheaper and easier to produce content and publish it.

It has also enabled virtual communities to emerge across geographical distances and time zones. One of the most significant opportunities for free expression online is the ability to reach and connect with specific niche audiences. This is particularly important for individuals living in environments where they are not free to speak openly in person.

“It is the ability to connect with others, not just receive information, which has served as the internet’s true democratizing element, and is a major asset to free expression,” says Laura Tribe, a Canadian activist on freedom of expression.

In Sri Lanka, the web represents the last frontier for freedom of expression. Sri Lanka’s is a society where access to the mainstream media is carefully guarded by their gatekeepers (editor and owners) many of whom do not stand for the public interest and instead promote various private agendas or engage in excessive self-censorship. Against this backdrop, the web provides an extremely important alternative space for citizens. Many have seized the opportunity to discuss various topics of public interest that are often under-reported, ignored or blocked out in the mainstream media.



“THE OPEN FLOW OF INFORMATION HAS BEEN KEY TO THE INTERNET’S TRANSFORMATIVE EFFECT IN MODERN SOCIETY. IN ORDER TO SAFEGUARD ITS BENEFITS, THE RIGHT TO FREE EXPRESSION MUST BE DEFENDED WHEN ADDRESSING ISSUES OF CONTENT AND DEFINING THE TECHNICAL MANAGEMENT OF THE INTERNET’S ARCHITECTURE.”

ARTICLE 13 (ADVOCACY ORGANIZATION)
https://www.article^{19}.org/issue/digital-rights/

HATE SPEECH: MISUSE OF FREEDOM OF EXPRESSION

Freedom of expression is not an absolute right – some reasonable limits apply. One category of expression that is not allowed is hate speech.

Containing hate speech everywhere – both online and offline – involves a fine balancing act as overzealous regulation can easily trample on freedom of expression guaranteed by the Constitution of Sri Lanka, as well as international human rights treaties Sri Lanka has signed.

Hate speech has various definitions but is generally understood as the advocacy of hatred based on nationality, race, religion, gender identity or sexual orientation. Importantly, hate speech is different from offensive speech, and the two should not be conflated. Indeed, the right to FOE extends to unpopular ideas and statements which may "shock, offend or disturb." As author Salman Rushdie once remarked, "What is freedom of expression? Without the freedom to offend, it ceases to exist."

Hate speech in Sri Lanka needs to be understood in the context of the civil war, and the slow reconciliation since the war ended in 2009. The conflict heavily polarized Lankan society along ethnic, religious and political lines, and energized various forms of ultra-nationalism. Instead of nurturing national healing, political parties have only exploited these divisions. [See also Case Study 1 at the end of this module.]

Sri Lanka does not face a gap in the law as far as hate speech is concerned. In fact, the current law is fully compliant with international standards. The problem is one of enforcement. In countering hate speech, it is vital to allow legitimate criticism and dissent.

A global study by UNESCO noted in 2015 that “any limitations [to hate speech] need to be specified in law, rather than arbitrary. They should also meet the criterion of being ‘necessary’ – which requires the limitation to be proportionate and targeted in order to avoid any restriction of legitimate expression...”

In that study, titled ‘Countering online hate speech’, UNESCO said: “International standards also require that any limitation of expression also have to conform to a legitimate purpose, and cannot just be an exercise of power. Besides for the objective of upholding the rights of others...these purposes can also be national security, public morality or public health.”

UNESCO has recommended several non-legal ways of responding to hate speech online. Concerned individuals can engage in peer-to-peer counter-speech, while civil society groups can monitor, document and analyse hate speech, and where warranted, report such evidence to the authorities for legal action. Advocacy groups can also campaign for greater vigilance by internet companies.

In the medium to long term, the real defences against hate speech can only be built inside human minds. This is where enhancing digital literacy and strengthening the online community’s capability to counter hate speech becomes crucial.

FACEBOOK'S DEFINITION OF HATE SPEECH

Facebook's rules, known as Community Standards, define hate speech as a "direct attack on people based on what we call protected characteristics – race, ethnicity, national origin, religious affiliation, sexual orientation, caste, sex, gender, gender identity and serious disease or disability". It also provides some protections for immigration status.

Source: https://www.facebook.com/communitystandards/

WEB CENSORSHIP

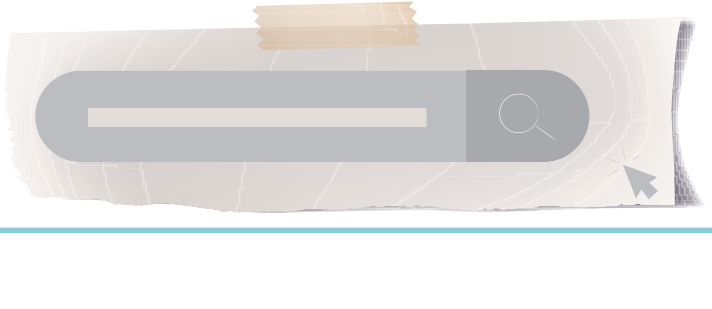
The internet was created to be an open platform. The liberal approach to its governance is rooted in the notion that an open and accessible internet is fundamental to the success of open and democratic societies.

However, as the internet's uses (and misuses) increase in both intensity and complexity, its original and fundamental values are coming under sharp scrutiny. As the Open Internet for Democracy, an alliance of advocacy groups, says: "The increasing shift of political and social discourse to online platforms has led to a corresponding rise in the use of the internet as a tool that can silence dissent, promote violence, and perpetuate prevailing inequalities, including regarding access and use."

The internet's creators, who were mostly liberal-minded academics or technologists, envisioned their creation to be open and free. But as it expanded and evolved, it has given rise to many contentious – and as yet unresolved – debates on how to govern the internet.

Because of its design, the internet cannot be controlled by individual governments using national laws and regulations. But some states have devised ways to filter, monitor and otherwise block content, thereby manipulating the openness of the internet. Even some democratic states have considered or already implemented various restrictions in response to the potential legal, economic, and security challenges raised by digital media.

This has given rise to intense global debates on internet freedom and what should be its reasonable limits. Under international law, for example, blocking of websites on an administrative basis, particularly when the decision is made and the action is undertaken by a government body, is not a justifiable restriction on freedom of expression.



"THE INCREASING SHIFT OF POLITICAL AND SOCIAL DISCOURSE TO ONLINE PLATFORMS HAS LED TO A CORRESPONDING RISE IN THE USE OF THE INTERNET AS A TOOL THAT CAN SILENCE DISSENT, PROMOTE VIOLENCE, AND PERPETUATE PREVAILING INEQUALITIES, INCLUDING REGARDING ACCESS AND USE."-

OPEN INTERNET FOR DEMOCRACY

"AS MANY GOVERNMENTS ARE PRESSURED TO RESPOND TO CYBER THREATS, ONLINE HATE AND TERRORISM, EVEN RIGHTS-RESPECTING GOVERNMENTS MAY SEE A FALSE CHOICE BETWEEN SECURITY AND HUMAN RIGHTS. FOR EXAMPLE, EFFORTS TO UNDERMINE ENCRYPTION OR BAN ANONYMIZING TOOLS LIKE TOR FOR NATIONAL SECURITY PURPOSES THREATEN FREE EXPRESSION AND PRIVACY OF INDIVIDUALS EVERYWHERE. WHILE NEW TECHNOLOGIES CAN OFFER THE PROMISE OF MORE EFFICIENCY AND NEW SERVICES, THEY CAN ALSO BE USED BY GOVERNMENTS — IN THE NAME OF SECURITY – TO CREATE A SURVEILLANCE SOCIETY, UNDERMINING FREEDOMS AND PRIVACY."

GLOBAL INTERNET REPORT 2017
BY THE INTERNET SOCIETY

RIGHT TO PRIVACY

The right to privacy is also enshrined in the UDHR (in Article 12), and subsequent international conventions. Today, our increasingly digital lives and greater use of online services have added a new layer of complexity to privacy protection.

Advances in information and communication technologies (ICTs) have dramatically improved real-time communication and information sharing. At the same time, these technologies are vulnerable to unauthorized interception, electronic surveillance and data mining.

Absolute privacy protection is not possible online: every action is automatically documented somewhere and is ultimately traceable. Within this reality, however, reasonable levels of privacy controls are still feasible. But ensuring that it actually happens is a shared responsibility of technology service providers, technology users and governmental regulators.

Unfortunately, many users of online services are unaware of multiple privacy pitfalls online, and some of them inadvertently compromise their own privacy.

One major challenge when it comes to cyber space interactions is that the demarcation between public and private lives is blurred or lost. This is especially the case in social media, where both private space and public space co-exist and often overlap.

[9] https://openinternet.global/about-open-internet-democracy-initiative

DIGITAL RESPONSIBILITIES

"With great power there must also come great responsibility!" is a well known quote that was originally made popular by the Spider-Man comic books.

This advice is very apt for every user of digital technologies and the web: with the power to access so much information and to communicate so widely and so fast comes a great responsibility to behave well while doing so.

This is a personal responsibility for every individual. It has been expanded in different ways. In one discussion, the key responsibilities have been listed as follows:

- Responsibility to report bullying, harassing, sexting, or identity theft
- Responsibility to cite works used for resources and researching
- Responsibility to download music, videos, and other material legally
- Responsibility to keep data/information safe from hackers
- Responsibility not to falsify your identity

In another discussion of the topic, the following personal responsibilities have been associated with becoming a productive digital citizen:

- Cyberbullying: You are responsible for how you interact with other digital users. And you are also responsible for protecting yourself against abusive relationships.

- Internet safety: Personal safety should always remain a top priority. Many users wrongly believe that internet safety is all about children, cyber-bullying and sexual predators – but it covers much more, and everyone should take basic precautions.

- Netiquette or internet courtesy: Internet communication involves keyboard shortcuts, but sometimes the shortcuts can hamper understanding and professional exchanges. For example, typing entirely in capital letters is not a good idea as it is like “SHOUTING.”

- Reporting Offenders: Part of responsible Digital Citizenship demands that we deal with digital offenders in a manner that can end their offensive behaviour. It can be as basic as reporting/complaining to a platform about inappropriate content or cyber-bullying. Depending on the offence and situation, you may have to report to the legal authorities.

- Legal protection: Protecting yourself online involves learning the laws that govern internet activities in your country. For example: Do you know and understand digital copyright regulations? Are you familiar with websites that involve software pirating? How can you prevent someone from stealing your digital identity?

TREATING THE INTERNET AS A NEIGHBOURHOOD

Jacqui Murray, a school teacher in the US who has been teaching technology for middle school children for over 20 years, has suggested this approach to digital responsibility:

Think of the internet as having comparable expectations to a neighborhood:

- Act the same way online as you'd act in your neighborhood.
- Don't share personal information. Don't ask others for theirs. Respect their need for privacy.
- Be aware of your surroundings. Know where you are in cyberspace. Act accordingly.
- Just as in your community, if you are kind to others, they will be kind to you.
- Don't think anonymity protects you -- it doesn't. You are easily found with an IP address. Discuss what that is.
- Share your knowledge. Collaborate and help others online.

Source: https://www.teachhub.com/technology-classroom-digital-rights-responsibilities

CASE STUDIES

CASE STUDY 1: HATE SPEECH ON FACEBOOK IN SRI LANKA

Warnings of hate speech spreading online have been sounded for several years. A few concerned social activists and researchers have been gathering and analyzing evidence of rising volumes of hate speech, especially on Facebook.

In the first such local study in 2014, the Centre for Policy Alternatives (CPA) noted: "The growth of online hate speech in Sri Lanka does not guarantee another pogrom. It does however pose a range of other challenges to government and governance around social, ethnic, cultural and religious co-existence, diversity and, ultimately, to the very core of debates around how we see and organise ourselves post-war."

Titled Liking Violence: A study of hate speech on Facebook in Sri Lanka, the report looked at 20 Facebook groups in Sri Lanka over a couple of months, focusing on content generated just before, during and immediately after violence against the Muslim community in Aluthgama in June 2014. More generally, the study explored the phenomenon of hate speech online – how it occurs and spreads online, what kind of content is produced, by whom and for which audiences.

While the Muslim community in Sri Lanka – who make up 9 per cent of the population have been the direct target of most such online hate speech, the CPA study found various other groups are also being targeted. Among them were human rights activists, moderate politicians, clergy who advocate religious harmony, women, LGBT community and many citizens who don't 'identify with the hardline Sinhalese Buddhist cause'.

“Ultimately, there is no technical solution to what is a socio-political problem,” say CPA’s researchers Shilpa Samaratunge and Sanjana Hattotuwa. That sums up the challenge: the massive number of users, high level of content volume and diversity, and the speed at which hate speech is being generated and shared make real time monitoring a daunting task.

The challenge is complicated by some governments trying to stifle political criticism in the guise of curbing hate speech.

More: https://www.cpalanka.org/liking-vilence-a-study-of-hate-speech-on-facebook-in-sri-lanka/

CASE STUDY 2: INTERNET SHUTDOWNS AND SOCIAL MEDIA BLOCKINGS

Network shutdowns -- defined as intentional restrictions on connectivity for fixed-line internet networks, mobile data networks, or both -- have occurred in a growing number of countries in recent years. These seriously disrupt citizens' right to information and communication.

In most cases, governmental authorities do not disclose clear reasons for such shutdowns. Where reasons are given, they can be sorted into a few broad categories: to maintain national security; to ensure the integrity of elections; to contain protests and demonstrations; or to prevent cheating at key school or public examinations.

Internet shutdowns need to be seen as part of a wider set of factors undermining internet freedom. Freedom House, an international advocacy organization promoting freedom of expression, has documented a decline in internet freedom for the past seven years since 2010. Their annually published report, Freedom on the Net, is a comprehensive study of internet freedom in 65 countries around the globe -- covering 87% of the world's internet users. It tracks improvements and declines in government policies and practices each year.

As Freedom on the Net 2018 report noted, "Shutdowns are a blunt instrument for interrupting the spread of disinformation online. By cutting off service during such incidents, governments often deny entire cities and provinces access to communication tools at a time when they may need them the most, whether to dispel rumors, check in with family members, or avoid dangerous areas."

As internet shutdowns and restrictions became more frequent, their economic, societal and political impacts have also increased – and been analyzed by various research and activist groups.

“Internet shutdowns have far-reaching rights, economic, and technical impacts. They undermine users’ trust in the Internet, setting in motion a whole range of consequences for the local economy, the reliability of critical online government services and even for the reputation of the country itself. Policymakers need to consider these costs alongside security imperatives,” noted the Internet Society (ISOC), in a public policy briefing in November 2017.

Up to June 2019, Sri Lanka has had four social media blocks. The first was in March 2018 during anti-Muslim violence in the eastern and central provinces. Then following the Easter Sunday terror attacks on 21 April 2019, the government blocked key social media platforms on three occasions for a total of 16 days. The efficacy of these blocks has been widely debated as many users found work-arounds through virtual proxy servers (VPN), and data analyses have shown that there was no significant drop in hate speech or misinformation – the reasons cited for blockings.

More at: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism
https://www.internetsociety.org/wp-content/uploads/2017/11/ISOC-PolicyBrief-Shutdowns-20171109-EN.pdf

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- The divide between online (cyberspace) and offline (physical space) is not very sharp anymore as there is more and more overlap. Discuss this in relation to your own experiences in using digital technologies and the web.
- Discuss the Universal Declaration of Human Rights with particular attention to Article 12 (which covers the right privacy) and Article 19 (right to freedom of opinion and expression).
- The right to FOE extends to unpopular ideas and statements which may "shock, offend or disturb" some persons. Do you agree?
- What are the main challenges of countering hate speech online? Is criticism of politicians and governments a form of hate speech? Discuss.
- How are digital privacy, surveillance and encryption inter-linked? Since absolute private is not possible online, what are some of the practical safeguards every user can take to protect digital privacy as much as possible?
- Study the 17 Feminist Principles of the Internet and identify how they contribute to a safer, more responsible and productive web use by everyone.

- ‘Freedom on the Net’ is an annual study of internet freedom around the world, produced by the US advocacy group Freedom House. Study the latest Freedom on the Net report and discuss whether your agree with their assessment of your country. https://freedomhouse.org/report-types/freedom-net

- Governments (including Sri Lanka’s) have resorted to total internet shutdowns or selective blockings of social media platforms and/or chat application platforms in the name of national security, law and order, elections integrity, etc. Is such indiscriminate blocking justified under any circumstances? Discuss.

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- All digital rights are human rights as they apply in cyberspace. The promotion of these rights is closely linked to what happens in the physical world.

- Some human rights are particularly relevant in cyberspace. These include the right to freedom of expression, the right to data protection and privacy, and freedom of association.

- While basic access to the internet has vastly increased in recent years (more than half of global population was using it by 2018), connecting the rest remains an important goal.

- Digital and web tools are double edged. They can enable the fulfillment of human rights but can also be used to limit access to information through content blocking and full-scale internet shutdowns, or stifle expression through surveillance.

- Hate speech is found both offline and online, and societies need to respond to both in the same manner: allowing legitimate criticism while countering expressions that can lead to real world harm.

- Laws against hate speech are necessary but not sufficient. Among the non-legal strategies are civic education, enhancing digital literacy, and strengthening the online community’s capability to engage in counter-speech.

- The internet was created to be an open global platform. Its design makes it impossible for any government to control it, but some governments have devised ways to filter, monitor and otherwise block content within their countries.

- Civil society groups have provided thought leadership in evolving the global internet to be a more inclusive, gender sensitive, participatory and safer space. Over the years, this has been advocated through the Internet Rights Charter, Feminist Principles of the Internet and other key documents.

FURTHER READING

UN Human Rights Council's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
https://www.ohchr.org/en/issues/freedomopinion/pages/opinionindex.aspx

UN Human Rights Council's Special Rapporteur on the right to privacy
https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

Freedom on the Net: An annual study of internet freedom around the world
https://freedomhouse.org/report-types/freedom-net

2017 Global Internet Report: Paths to Our Digital Future. The Internet Society, 2017.
https://www.internetsociety.org/globalinternetreport/

Association for Progressive Communications (APC)
https://www.apc.org/

Liking violence: A study of hate speech on Facebook in Sri Lanka
Centre for Policy Alternatives, 2014.
https://www.cpalanka.org/liking-violence-a-study-of-hate-speech-on-facebook-in-sri-lanka/

Article 19 (freedom of expression advocacy organization) digital rights archive:
https://www.article19.org/issue/digital-rights/

Electronic Frontier Foundation (EFF)
https://www.eff.org/

Council of Europe freedom of expression website
https://www.coe.int/en/web/freedom-expression/internet-freedom1

Two sides of the same coin – the right to privacy and freedom of expression
An exploration by Privacy International
https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression

MORE RESOURCES

EROTICS: An online network of activists and researchers working on the intersections of sexuality and the internet.
https://erotics.apc.org/

Gender and Internet Governance eXchange: Addressing the gap in participation by women's rights and sexual rights advocates in internet governance policy processes and development
http://gigx.events.apc.org/en/home-page/

Gender Evaluation Methodology: How to evaluate ICT projects thinking about gender
http://www.genderevaluation.net/

GenderIT.org: The world's first website focusing on gender and technology policy
https://www.genderit.org/

Take Back the Tech! A call to take control of technology to end violence against women
https://www.takebackthetech.net/

MODULE 2

DIGITAL COMMUNICATION

MODULE 2

DIGITAL COMMUNICATION

We humans are highly communicative creatures. We have evolved languages and media as means of communicating with each other.

We not only like to share information and opinions but also weave them into narratives. This makes us story tellers. Story telling is as old as human civilizations.

Today's digital tools and the web provide many opportunities for communicating fast and to a wide audience. Any individual with a basic access device like a smartphone and an internet connection can express herself to the whole world through blogs, social media, podcasts and other means.
This has democratized communication. With such great power comes great responsibility.

Communication is not only self-expression. It is also a tool for researching information, organizing and mobilizing people and building communities. Using digital communications, people living in locations far apart or across different time zones can connect, share and collaborate.

Communicating is ideal when it is a two-way process. Mass media (mostly) involves one-way communication from content producers to their audiences. In contrast, communications online can happen in both directions: the web enables easy interaction and participation. It is up to everyone who gets online to use this facility with a sense of purpose, imagination and courtesy.

An important element of communication is the art of listening. Being able to exchange information and opinions in real time is useful, but it sometimes makes us react without enough reflection. We may sometimes regret what was said in the heat of an argument in social media.

In this module, we cover a few basics in communicating effectively and ethically using digital tools. Please consider it as a rough guide to more thoughtful and responsible digital communications at both private and public levels.

KEY TERMS

Digital communication can mean different things to different people.

In a technical sense, it means enabling successful transmissions and reception of signals using digital communication facilities – whether in telecommunications, broadcast or internet.

Digital communication also means individuals and groups communicating their messages using digital technologies and the web. Such communications can be private or public.

Digital storytelling refers to various forms of digital narratives, e.g. web-based stories, interactive stories, narrative computer games, audio and video podcasts, etc. A digital storyteller can be anyone who has a desire to document life experiences, ideas, or feelings through the use of story and digital media.

Strategic communication explores the capacity of all organizations—governments, corporations as well as advocacy and activist groups and for engaging in purposeful communication.

DIFFERENT FORMS OF DIGITAL COMMUNICATION

Digital communication methods, tools and platforms have been expanding over the years. Here are the more commonly used ones:

- **INTERNET** is the world's biggest communication network of computers. It connects millions of smaller domestic, academic, business and government networks, which together carry many different kinds of information. The name is sometimes abbreviated as the net.

- **WORLD WIDE WEB ("WWW" OR "THE WEB")** is the prominent part of the internet that contains websites and webpages. It was invented in 1989 by Tim Berners-Lee by creating a new system called HTML. Websites are composed of pages linked by hypertext links. They are written in HTML.

- **ELECTRONIC MAIL (EMAIL)** is an internet service that allows people who have an email address (account) to send and receive electronic messages. Those are much like postal letters but are delivered much faster.

- **VOICE OVER INTERNET PROTOCOL (VOIP)** is a method that allows voice calls over the internet. The best known service is Skype. Using VOIP reduces costs:it does not require a dedicated line as in telephone services. Today many VoIP services allow both voice and video, but the video option consumes more data.

- **MOBILE PHONES** (also known as handphones, cell phones, or cellular telephones) are small portable telephones that allow us to communicate with others anywhere and anytime (provided there is signal coverage). In developing countries in Asia, mobile phone markets are still dominated by basic handsets for voice calls and texting, with no (or very limited) internet access capability. A feature phone, in comparison, has additional capabilities for multimedia (such as photos and music) and internet browsing. To be called a smartphone, however, the instrument must use an operating system such as Android or iOS through which third party 'apps' could be run on it. Smartphones usually come with a touch screen covering at least 75% of its front area. All smartphones can access internet.

- **SOCIAL MEDIA** are a category of websites, web platforms and apps based on user participation and user-generated content. They allow users to interact with each other, as well as to produce, present and promote content. They enable users to engage with audiences that are local, national, regional and global. While social media includes web forums, wikis and blogs, the term is most often used today to describe social networking websites such as Facebook, Instagram, YouTube, Pinterest and Twitter. In recent years social media have been fueled by the spread of smartphones.

- **INSTANT MESSAGING (IM)** a type of online chat that offers real-time transmissions over the internet. Some IM applications can use push technology to provide real-time text, which transmits messages character by character, as they are composed. More advanced instant messaging can add file transfer, clickable hyperlinks, Voice over IP, or video chat. There are many IM services available today, some of which are attached to social networking sites. However, each IM service offers its own proprietary software client as a separate program or as a browser-based program. Among the popular IM services in Sri Lanka are WhatsApp, Viber and Facebook Messenger.

- **SMS (SHORT MESSAGE SERVICE)** is a text messaging service component of most telephone, internet, and mobile device systems. It uses standardized communication protocols to enable mobile devices to exchange short text messages of a limited number of characters. In recent years SMS use has been declining as the more versatile instant messaging services gain in popularity. But SMS still remains an important technology, for example, in location-based alerting for delivering disaster early warnings.

- **BLOG** is a website that contains information and opinions, usually by a single author, known as a blogger. Prior to blogs, users needed to know coding like HTML to produce a website or they had to get help from someone who did. But blogs opened up online publishing to anyone with internet access by offering content management systems that are easy to use. While personalized blogs dominate the blogosphere (that is, the entire space of blogs), there are also group blogs involving multiple contributors. Some institutions maintain a blog for free discussion of ideas in addition to their own website.

INTERNET AND WEB ARE NOT THE SAME

The terms internet and web (short for world wide web or www) are used interchangeably, but they are not the same thing. They are linked but separate phenomena. This is how American computer scientist Vint Cerf, one of the 'fathers of the internet', explains the difference: "The internet is the underlying networking infrastructure that links billions of computers all around the world. The world wide web is an application that sits on top of the basic internet infrastructure. The two are simply layered on top of each other. What you'll experience of the internet, for the most part, is through the world wide web." The internet was developed from the 1960s to allow multiple computers to communicate on a single network. It started in the US and later involved European institutions as well. But the internet remained confined to 'techies' who knew computer programming (or coding) until the easier to use web emerged in the early 1990s largely thanks to the work of British computer scientist Tim Berners-Lee.

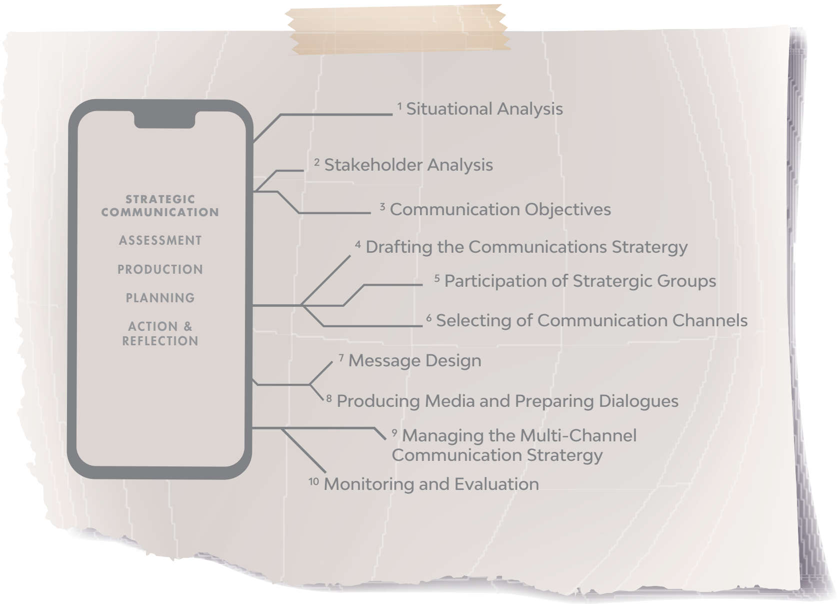
More: https://www.webopedia.com/DidYouKnow/Internet/Web_vs_Internet.asp

There are many digital and web-based tools to choose from, including what we have listed above. Most of them are available free of cost for those who sign up or open a user account with the various services.

However, this increased choice does not mean you have to use all or even most of them. Now, more than ever before, we need to be selective and strategic about how we communicate – or we risk just expressing ourselves without being sure if anybody is listening or engaging us.

This is where strategic communication becomes important – it is described as "the purposeful use of communication by an organization to fulfill its mission".

In strategic communication, message development, or the process of creating key points or ideas, involves high levels of planning and research. These messages are targeted or created with a specific audience in mind (at least a clearly defined primary audience, while everyone else can be secondary audience).


STRATEGIC COMMUNICATION
ASSESSMENT
PRODUCTION
PLANNING
ACTION & REFLECTION
1 Situational Analysis
2 Stakeholder Analysis
3 Communication Objectives
4 Drafting the Communications Stratergy
5 Participation of Stratergic Groups
6 Selecting of Communication Channels
7 Message Design
8 Producing Media and Preparing Dialogues
9 Managing the Multi-Channel Communication Stratergy
10 Monitoring and Evaluation

As seen in this diagram, strategic communication involves four stages (each of which has several actions):

- ASSESSMENT, i.e. understanding what needs to be communicated to whom
- PLANNING which involves deciding how best to engage the chosen audience/s
- PRODUCTION of messages and materials (which comes only after the above two stages)
- ACTION AND REFLECTION involves disseminating, engaging and evaluating that experience

The principles of strategic communications are relevant for both digital and non-digital communications. Having a clear sense of purpose is essential for any form of public communication whether it is for political campaigning, social activism or product marketing.

The word "communication", comes from the Latin ***communicare*** (which means to share or to make common) and ***communis*** (belonging to all). Both terms are also related to the word "community".

A helpful and non-technical guide to strategic communications is at: https://www.jrmyprtr.com/comms-101/

DIGITAL ETIQUETTE

The idea behind digital etiquette (also called internet etiquette or netiquette) is "treat others how you want to be treated."

It means respecting other users' views and displaying common courtesy when posting your own views online, and when interacting with others.

There are appropriate and inappropriate ways to behave and treat one another online, just as there are proper and improper ways related to treating others offline. Your choices of words and actions in the digital world can have an impact on others. It defines what kind of person others perceive you to be.

Here are three common examples:

- Imagine you are at a theatre for a movie or play. Somebody's mobile phone rings. Instead of turning the phone off (which should have been done at the beginning of screening or performance), s/he engages in a loud conversation – disturbing everyone around. That certainly should not happen.

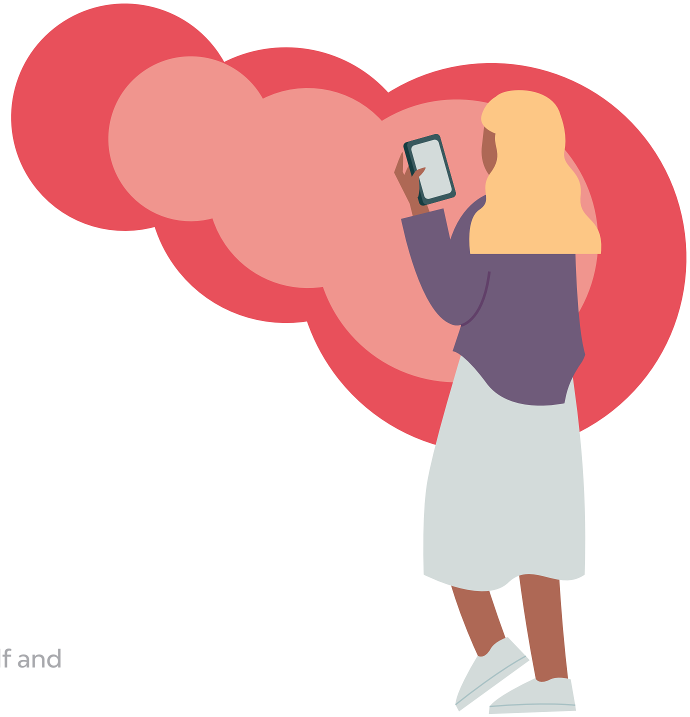
- You are having a conversation with a family member, friend or colleague – and also keep checking your mobile phone and responding to incoming texts or instant messaging. Your attention is thus divided between the person in front of you and someone online. This is rude behaviour, and a sign of poor time management too.

- In an email exchange or social media conversation, wishing to emphasize some points you type text entirely in upper case or CAPITAL letters. You mean no harm, but it can be considered "shouting" and therefore rude. Netiquette discourages the use of all capitals when posting messages or in emails. All capitals can be used for a single word or phrase to express emphasis, but NOT for a whole sentence or paragraph (this sentence itself is an example of how to do it right)

In the above examples, the first one involves behaviour that is not permitted in many theatres and cinemas – the offender could be hushed down by others around, or even be asked to leave by the theatre management. The second and third examples are actions that break social norms rather than any institutional rule.

There are many do's and don'ts that should be practiced when interacting online, and when using digital tools. It is not possible to provide a list here; many online guides and resources are available with such advice.

One thing to remember: adhere to the same standards of behavior online that you follow in real life. Respectful and ethical behaviour matters both online and offline.



[2] See, for example, https://uncw.edu/oel/documents/pdfs/netiquette.pdf and https://www.verywellmind.com/ten-rules-of-netiquette-22285

DON'T FEED THE TROLLS!

In internet slang, a troll is someone who tries to cause discomfort or distress in others. Trolls sow discord and create 'drama' needlessly to gain attention for their own amusement by posting inflammatory, extraneous, off-topic messages with the deliberate intention of provoking readers into an emotional response.There are various types of trolls – those who simply poison public discourse, as well as those who freely express derogatory or discriminatory views under the name of "free speech" (which has certain limits). Not all controversial or unpopular comments are the work of trolls, as radically disagreeing opinions can sometimes stimulate useful discussion. For this reason, it is not always easy to tell whether someone is trolling or being simply very opinionated.How to deal with trolls? The best advice: ignore them, rather than giving them the satisfaction of any attention or reaction. If you don't feed the trolls, they'll probably leave you alone.

Source: https://theconversation.com/dont-feed-the-trolls-really-is-good-advice-heres-the-evidence-63657

WITH ALL DIGITAL MEDIA, BE RESPECTFUL, AVOID ANGRY OUTBURSTS AND BE CAREFUL HOW YOU USE SATIRE OR POTENTIALLY INAPPROPRIATE HUMOUR. WHAT WORKS IN PERSON OR EVEN BY PHONE SOMETIMES DOESN'T WORK WELL ONLINE BECAUSE THE HUMAN CONTACT THAT PUTS THINGS INTO CONTEXT IS OFTEN MISSING. AND REMEMBER, ANYTHING YOU POST OR SEND IN AN E-MAIL OR EVEN TEXT MESSAGE CAN FOREVER BE COPIED, STORED OR FORWARDED. SOMETHING YOU POST OR SEND TODAY CAN HAUNT YOU FOR YEARS." -

LARRY MAGID, IN DIGITAL ETIQUETTE FOR THE
21ST CENTURY

UNDERSTANDING MOBILE JOURNALISM

Mobile journalism is a form of digital storytelling where a smartphone is the primary device used for creating and editing images, audio and video. Both professional journalists and citizen journalists can benefit from this practice.

One definition for mobile journalism is this: “a new approach for media storytelling where reporters or activists are equipped for being fully mobile and fully autonomous”.

Smartphones are at the heart of mobile journalism, and are increasingly used by journalists for radio news and podcasts, and video for TV news and documentaries as well as videos for social media platforms.

More than any other device, smartphones encourage cross-platform creativity and digital innovation. Photos, videos, audio and graphics can be created and edited on the phone and uploaded to news media websites and/or social platforms directly. You can also respond to audience queries and contacts via chat apps, social messaging and email.

A smartphone can put a complete production studio for radio, television, text and social content in your pocket. Here are a few reasons to take up mobile journalism.

- **Affordable:** You can achieve TV-quality video by combining a good quality smartphone with an external microphone, a tripod and tripod mount, and by using a professional video recording app. This set-up is significantly cheaper than a traditional broadcast quality video camera.
- **Portable:** Most mobile journalists can fit their equipment in a backpack. The phone plus a lightweight tripod, clip-microphones and an external light can weigh under 3kg, making it easy to produce high quality stories anywhere, anytime.
- **Discreet:** The fact that smartphones are so commonplace makes them a valuable tool for journalists who need to operate discreetly.
- **Approachable:** The small size of smartphones, and the fact that they are so commonplace, means they are less intimidating for interviewees. A study by the Reuters Institute of Journalism found that people are more likely to agree to an interview and to open up in front of a smartphone than in front of a larger TV camera.
- **Apps for beginners to professionals:** There are dozens of storytelling apps for iPhones and Androids. Some are simple and designed for quickly creating social stories with animated titles, fun captions and free music. They are also fast to learn and use, so they're ideal for creating a great-looking story on a deadline.

TIPS FOR USING KEY SOCIAL MEDIA

Twitter

- Use hashtags to gain traction – standard ones such as #LKA and #SriLanka will let your message be seen by those who follow Sri Lanka related content. Also important to choose short yet impactful hashtags for any of your campaigns, so those engaging can all literally be on the same page – hashtags allow you to collate campaign information better as well.

- Make use of Twitter moments to bring all your tweets, and related tweets, from one campaign or story into a single thread.

- Method of crowd-sourcing information – tweeting out requests for opinions/ observations allows you to make articles/write-ups richer with a wider range of voices contributing to your work.

- Use photos in your tweets, and direct players for any video/audio content. Twitter currently (as at mid 2019) allows video uploads of up to 2.20 minutes. In addition, YouTube and SoundCloud links allow for playing within the tweet itself, which is convenient for users and therefore likely to be watched/listened to more.

Facebook

- Upload any videos that you make directly to Facebook – this gives a better in-app playing experience than external links.

- Use photos in your posts and make albums for key events/campaigns/topics that include links to work on other platforms [including article link, link to Twitter hashtag].

Instagram

- Visual content is moving content; a well-captured image and informative caption can have more impact than a long, analytical article.
- Targets young people who are largely active to Instagram – they use it as their main hub for information, influence and interaction.
- Important to post regularly and to use hashtag in captions – include all hashtags after actual text so that it is less cluttered for your viewer.
- Tag individuals doing similar work/with similar interests in your posts – human rights groups, citizen journalists, etc.
- Use stories if reporting live or on a key issue, and hashtag your story with general tags such as #LKA, #SriLanka too.

In the end, however, what matters more than having the latest tech gadgets or accessories is for you to have a clear idea of what you want to communicate to whom and why.

SAFE AND ETHICAL DRONE USE

Unmanned aerial vehicles (UAVs) or drones were best known for being used for military purposes. But in recent years they have become a civilian tool being used for many peaceful purposes. The cost of drones has also come down (an entry level unit sells for around LKR 30,000 in Colombo) while their versatility increased. This has spurred many new uses – from newsgathering and post-disaster assessments to goods delivery and smart farming.

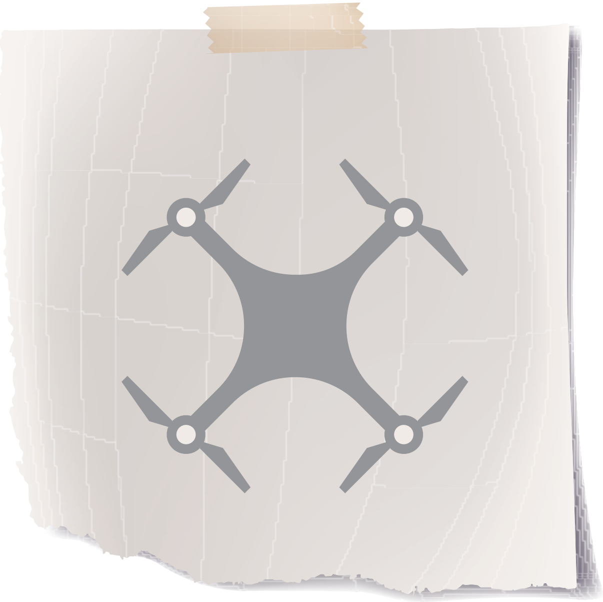
In Sri Lanka, wedding photographers, TV journalists and political parties were among the early adopters of drones. They grasped the value of the 'bigger picture' perspective aerial photos or videos provide – it helps journalists and activists to make sense of complex situations like climate change impacts, resource conflicts, or political agitations. Drone-obtained visuals can enhance field-based reporting and investigative journalism.

Beginning in 2016, a few dozen journalists and photojournalists have been trained in drone-assisted journalism by drone journalism enthusiast (and drone pilot) Sanjana Hattotuwa and journalist Amantha Perera. Using the bird's eye view, some have done good stories such as probing drought's impacts in the dry zone, rising garbage crisis in Kattankudy on the east coast, and taking a closer look at land use patterns in Hambantota.

But drones can also be misused in ways that violate people's privacy and threaten public safety. Already some news organisations have used drones without due regard for public safety or media ethics. Example: a drone hovered over the Colombo general cemetery as slain journalist and editor Lasantha Wickrematunge's body was exhumed in September 2016 – against the wishes of the family that had asked for privacy.

The Civil Aviation Authority of Sri Lanka (CAASL) has published regulations for drone operation for all users including journalists. While drones below 1 kg don't need registration with CAA, those between 1 and 25 kg do (and those over 25 kg are not permitted to fly). Even those registered cannot be flown over some specified areas which includes congested areas, roads or railway lines, national parks and security zones. The drone pilot must always maintain visual line of sight.

"We request all those who fly drones to do so with the awareness that while they may be seen as toys, in their actual use and operation, they can lead to hurt, harm and litigation if inappropriately deployed. Respecting ethics, privacy and being mindful of the safety of those under and around the theatre of flight operations must be paramount," says a statement issued by the Ministry of Mass Media in January 2017.



Code of Ethics for Drone Journalists formulated in the United States is available at : http://www.dronejournalism.org/code-of-ethics/

[3] Ministry of Mass Media statement on drone use: http://www.aviationvoice.lk/drone-journalism-sri-lanka-ethics-regulations-guidelines/

CASE STUDIES

CASE STUDY 1: DIGITAL STORY-TELLING IN JAFFNA

A decade after the civil war ended, residents of Sri Lanka's Northern Province are rebuilding lives, livelihoods and communities. Entrepreneurship is spreading. Civil society is resurgent. Despite this, mainstream media still peddles stereotyped narratives, most of it negative.

"Countering foreign media that tends to stereotype us is one thing, but the content in local media too is very troubling. It thrives in polarizing our people," says young journalist and digital activist Benislos Thushan, a native of Jaffna.

This motivated him to train fellow youth in digital story-telling (DST). Already, 10 batches of young men and women have completed the six-month course that is offered free and held at the American Corner in Jaffna.

"Almost 200 students have come out of this training programme [up to mid 2019] and we are constantly updating our modules," says Thushan. "Everybody has a smartphone and likes taking pictures. But being a citizen journalist comes with greater responsibility.

"Thushan, who has worked for newspapers and also been part of peace-building initiatives, is employed in Colombo during the week and travels to Jaffna (400km north) every Friday night to conduct his classes in Jaffna during weekends.

"The aim of the DST course is to build digital story telling competencies among our youth and to promote citizen journalism," says Thushan. "By now most young people have access to smartphones. They have connectivity. Most of them love taking photos with their phones. They love sharing their stories too, but they lack guidance...My classes encourage young people to venture beyond and experiment with the digital tools they already have.

”The DST course covers the fundamentals of story-telling, photography as a visual story-telling tool, and use of social media. Participants are also taught media ethics, protecting anonymity of sources or photo subjects when requested, and being sensitive to political realities.

Every participant has to do a photo essay on a topic of her choice. Many interesting and innovative projects have emerged – some being continued online as voluntary efforts.

One participant has set up ‘Everyday Mullaitivu’ Facebook page that shares photographic vignettes of life in his area (one of Sri Lanka’s least developed districts). He features stories of positivity coming out of Mullaitivu.

Another started ‘Jaffnapedia’ with a friend. Using Instagram and Facebook pages, they seek to capture everyday sights of Jaffna’s people and places. They also invite others to send photos, which the two curators selectively share.

Thushan says: “Story telling is empowering. When you can tell stories from your own communities, you can substantially reduce the polarization caused by (mainstream) media. We want to be recognized not just a region of post-war, but also as communities with lots of hope. People are striving hard to overcome the past.

”He adds: “Those who tell our story have the power to shape that narrative. We lose our power when we lose our narrative.”

More: https://www.thehindu.com/news/international/going-beyond-the-scars-of-the-civil-war/article27950495.ece
https://www.facebook.com/DSTjourney/
https://www.facebook.com/everydaymullaitivu/
https://www.facebook.com/jaffnapedia/

CASE STUDY 2: SOCIAL MEDIA DECLARATION

Optimizing the benefits of social media and minimizing its misuses is the aim of the Social Media Declaration, a code of conduct for Responsible Social Media use in Sri Lanka adopted by 16 civil society groups in 2019.

It recognizes the importance of the freedom of expression on social media, yet at the same time, encourage and strengthen the ethical, progressive, democratic and pro-social use of social media.

As its dedicated website notes, "Discussion on 'Social Media' has come under scrutiny within the present Sri Lankan context. The resulting discourse on freedom of speech and human rights has demonstrated that there is a lack of understanding of the nuanced and complex nature of social media, democracy or freedom of expression, especially by those in decision-making positions.

"The voluntary Social Media Declaration is a civil society response to this need, intended to "create a guideline/declaration in this regard, and that it should come from within Sri Lankan media and civil society itself."

Its objective is "to foster a community that encourages the responsible use of social media and the strengthening of digital literacy to allow for the right to access and an information-based society. While acknowledging the potential for social media to be misused, this Declaration recognizes digital rights as intrinsic to a society founded on principles of social justice, human dignity and prominent human and social ideals, based on a human rights framework."

Signatories to the Social Media Declaration pledge to minimize and eventually eradicate the generation and spread of the following:

- Discrimination based on race, religion or caste.
- Gender-based violence (including sexism, sexual violence, misogyny and the non-consensual dissemination of intimate images and videos) and other forms of discrimination against women.
- Sexual abuse.
- Harassment based on sexual orientation or gender identity.
- Violation of child rights and child exploitation, including child abuse and trafficking.
- Content inciting hate or violence, threats, intimidation, cyber-bullying and dangerous speech.
- Harassing marginalised communities.
- Illegal acts.
- Data theft and unethical abuse of sources of information and media (such as using photographs without permission).
- False information, misinformation and disinformation.
- Irresponsible sharing of explicit sexual content.

The following entities have signed the Social Media Declaration (as listed on website):
Centre for Policy Alternatives, Eastern Province Journalist Forum, Groundviews.org, Hashtag Generation, Internet Media Action, Jaffna Press Club, Lanka News Web, Law and Society Trust, Maatram.org, Movement for Land and Agricultural Reform, Nelum Yaya Foundation, Outbound Today, PEACE ECPAT Sri Lanka, Rights Now Collective for Democracy, Sarvodaya Shramadana Movement, Sri Lanka Muslim Media Forum, Sri Lanka Working Journalists' Association, Transparency International Sri Lanka, and Vikalpa.org.

More: http://www.socialmedialanka.org/

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- An important element of communication is the art of listening. If you agree with this, what can be done to encourage more people to pause, reflect and then respond – rather than hurriedly participate in fleeting conversations online?

- Can you think of successful examples specific to Sri Lanka where strategic communication was used for social and public benefit?

- The discussion on digital netiquette has cited a few examples. What other examples illustrate good or bad online behaviour?

- Have you been trolled online, and if so, how did you deal with trolling?

- What would you do when you come across expressions of sexism or misogyny by your ‘friends’ in social media? Do you ignore or react (and if the latter, how?)

- Do you know of more examples of digital story-telling anywhere in Sri Lanka on any social, cultural, political or community topic?

- How is digital communication -- especially instant messaging and texting – affecting the use of language? Can you identify examples where words and phrases are abbreviated, local languages are mixed with English, and emojis enter conversations?

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- Today's digital tools and the web provide many opportunities for communicating fast and widely. With such great power comes great responsibility.
- Communicating is ideal when it is a two-way process. Unlike in mass media, online communications can happen in both directions, enabling better interaction and participation.
- An important element of communication is the art of listening – which we don't do enough in today's hurried digital communications. It helps to pause and reflect every now and then.
- We need to be selective and strategic about how we communicate – or we risk just expressing ourselves without being sure if anybody is listening or engaging us.
- Digital etiquette (internet etiquette or netiquette) means respecting other users' views and displaying common courtesy when posting your own views online, and when interacting with others. Adhere to the same standards of behavior online that you follow in real life.
- Mobile journalism is a form of digital storytelling where the primary device used for creating and editing images, audio and video is a smartphone.

FURTHER READING

Digital Storytelling: Featuring some of the digital stories produced by participants at various workshops they have facilitated over the years.
http://stories.apc.org/

Transformative storytelling for social change
https://www.transformativestory.org/

10 ways to improve your digital etiquette
https://www.theguardian.com/media/2019/mar/10/10-ways-to-improve-your-digital-etiquette

‘Don’t feed the trolls’ really is good advice – here’s the evidence!
https://theconversation.com/dont-feed-the-trolls-really-is-good-advice-heres-the-evidence-63657

Mobile journalism manual: Guide for newsrooms and reporters
http://www.mojo-manual.org/

MOJO: The Mobile Journalism Handbook
https://ethicaljournalismnetwork.org/mojo-the-mobile-journalism-handbook

Drone Journalism resources
https://gijn.org/drone-journalism/

MODULE 3

ENHANCING DIGITAL SECURITY

MODULE 3

ENHANCING DIGITAL SECURITY

The internet is a global network of computers that are inter-connected electronically in a way that they can exchange information.

To use a physical world analogy, the internet works like the postal system, but it delivers messages at the speed of light and is far more intricate. Just as the postal service enables people to send one another envelopes containing messages, the internet enables computers to send one another small packets of digital data.

Billions of different devices are connected to the global internet. Among them are supercomputers, personal computers (desktops, laptops or tablets), smartphones and other specialist devices produced by thousands of different manufacturers.

To be able to exchange data among these different devices, they all use a common 'language': a technical standard called TCP/IP (Transmission Control Protocol/Internet Protocol). And every device that connects also has an internet protocol or IP address.

When you post a letter, the postal system handles all the logistics: you don't need to know or worry about its collection, sorting, transporting and eventual delivery. Similarly, packets of internet data are transmitted through a variety of cables, routers and host computers on the way to their destination.

By the end of 2018, an estimated 3.9 billion people were using the internet along with tens of millions of entities that includes governments, companies, charities and other organizations. For the most part, their web using experience is safe and satisfactory. But when so many users and so many devices are connected, sometimes things go wrong. That is why digital security or cyber security is important.

Cybersecurity is about systems and things; cyber safety is about people. In this module we cover the basics of digital security (protecting your digital systems and devices). The next module on cyber safety covers the safety of persons when using digital services.

KEY TERMS

Digital security (also called Information Technology security or IT security): implementing systems to protect and safeguard information stored digitally. These devices may or may not be connected to the internet. In a computing context, security includes both physical security and cybersecurity.

Cybersecurity: Precautions taken to guard digital devices connected to the internet, especially to prevent unauthorized access to (or attack on) computer systems and data.

Cloud computing means storing and accessing data and programs over the internet instead of storing data on a computer's hard drive. The 'cloud' is only a metaphor for the internet.

Source: https://searchsecurity.techtarget.com/definition/cybersecurity

BASICS OF DIGITAL SECURITY AND CYBERSECURITY

When we use any digital system, we enter our data which can include personal data, confidential official data of organizations we work with, creative content and other kinds of data. When we connect to a network of computers – whether one within an organization or on the global internet – we come across other people's data.

It is necessary to protect our own data and devices, and also respect the security of others' data and devices. In an inter-connected network like the internet, everyone needs to pay attention to security because one user's weakness can affect everyone!

Digital security and cybersecurity is not just to guard against unauthorized access. We also need to be careful of accidental data damage or loss by ourselves or anyone else authorized to handle our data. Unforeseen events like floods, fires and electric power surges can also damage data.

Digital security and cybersecurity does not mean having highly complex security systems. Sometimes the best solution may not be very technical. It is also important to keep re-evaluating security practices as new threats keep emerging, especially on the internet.

Please remember: good digital security and cybersecurity requires user involvement, responsibility and vigilance. This is not something that can be 'outsourced' to a vendor that supplied the hardware or software, or to an IT professional or systems administrator.

It is not possible to list here all the steps necessary for digital security and cybersecurity – plenty of free advice is available online. Discussed below are a few basic tips, which represents a commonsense approach.

Source: https://wiobyrne.com/digital-hygiene/

DIGITAL HYGIENE MATTERS!

Digital hygiene is a term used to describe the cleanliness or uncleanliness of one's digital devices, accounts and data.

Good digital hygiene is important both at home and at work. A single compromised account or device could result in someone gaining access to your devices or accounts. If this is done maliciously, that means that someone could lead an attack on your data by stealing files, cracking passwords, hacking accounts, or worse.

HOW TO PROTECT YOUR DATA FROM COMPUTER VIRUSES AND MALWARE

Computer viruses are small programs that spread from one computer to another via emails, email attachments or accessories like USB drives. Viruses can modify or destroy any data and disrupt normal operation of the operating system.

- Use an up to date anti-virus program.
- Make sure your operating system (like Windows) and web browsers (like FireFox and Chrome) are up-to-date. Their latest versions will offer better protection.
- Be cautious with emails links: do not open unknown attachments or content (links) even from a known source.
- Use pop-up blocker for your browser.
- Use a pop-up blocker for your browser. Many pop-ups are spyware and adware that come with malicious payloads and can damage your system.
- Install a firewall: this is a program that screens incoming internet and network traffic. Along with your virus program, it can help prevent unauthorized access to your device.
- Password protect the administrator account.

Note: A device may not always show symptoms even if it is infected. Always perform regular system checks and virus scans to make sure your device is clean.

SYMPTOMS OF A VIRUS INFECTION

Here are a few common symptoms indicating a malware infection:

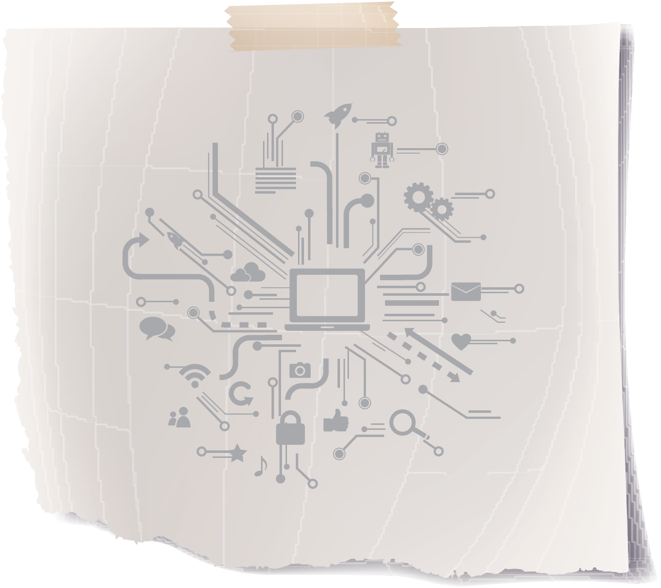
- The device will start to slow down without good reason.
- The device will abruptly restart itself often and will show abnormal behavior.
- Applications installed on the device will not function as expected.
- There might be unusual (typically badly written) error messages.
- There might be new shortcuts or other icons in the device that were not created by the user.
- Lack of storage space.
- Files or applications have been deleted without permission.

BACKING-UP DATA

Data corruption or loss can happen even with the best hardware and software. Data backup is a process of duplicating data to allow retrieval of the duplicate set after a data loss event.

A common data backup method is to download data from a computer's hard drive on to small portable devices like external drives or high capacity USB drives. There is also the option of backing up data remotely to the 'cloud' (web-based data storage, such as Google).

Cloud backup allows users to copy their data to hardware in a remote location. Users can access their data anytime on any device via the internet (when properly accessed). Cloud storage makes it easy to manage data. Most cloud storage service provide a large amount of storage space and encrypt the content for data security. (Some services providers like Google offer a basic online storage capacity for free when we sign up).



ENCRYPTING DATA

Encryption is the process of using an algorithm (automated software) to make data unreadable for unauthorized users. This protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text. Such data may only be decrypted or made readable with a ‘key’.

Encrypting data is like storing it in a safe - only those who have the access key can read it. Encryption is a digital form of cryptography, which uses mathematical algorithms to scramble messages, so that only those who have the sender's key (or cipher) can decode the message. Anyone else intercepting encrypted data will see junk.

There are two main methods of encryption: symmetric encryption, which involves securing data with a single private key, and asymmetric encryption, which uses a combination of multiple keys that are both public and private.

Encryption is especially important when communicating through the internet, e.g. email, chat applications and other exchanges. If messages are not encrypted, there are ways for malicious eavesdroppers to intercept or even alter the messages.

End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. It prevents potential eavesdroppers – including telecom providers, internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the digital exchange.

Encryption allows making your communication trusted and confidential. When it comes to end-to-end communication over the internet, example include services like WhatsApp, iMessage and Signal (in which E2EE is turned on by default) or Telegram.

DESTROYING SENSITIVE DATA

When you delete a file in your computer, it does not disappear completely. It only removes the reference of the file from the file system table. The file remains on the disk until another file is created over it, and even after that, it might still be possible to recover that data.

If you want to completely get rid of any data, it is best to use a secure deletion tool: it replaces or overwrites the sensitive information. Even after that, digital information could still be read by a skilled person who knows how to recover data.

A process called 'wiping' overwrites files with random data several times. Eraser is another advanced security tool for Windows, which allows users to completely remove sensitive data from the hard drive by overwriting it several times with carefully selected patterns.
Https://eraser.Heidi.Ie/

PROTECTING YOUR DATA WHEN ONLINE

Wi-Fi or wireless internet means connecting to a network using radio waves, without needing wires. It liberates users to remain connected to the internet as they move around, but this facility needs to be used with caution.

Public Wi-Fi can be found in public places like airports, coffee shops, shopping malls, restaurants and hotels — it allows you to access the internet for free. While it is ok to use public Wi-Fi to check social media or browse news articles, it is not advisable for reading email or accessing a bank account.

Why? Because using public Wi-Fi networks increases chances of your data being intercepted by someone else on that network. In fact, it is best to avoid Public Wi-Fi ‘hotspots’ that are run by people you do not know or trust. Criminals can set up hotspots known as 'evil twins' and 'rogue hotspots' to steal users' information.

Another precaution: always study privacy settings on social media platforms as well as other websites. You can often find privacy controls on a site by navigating to a control panel or settings menu. Privacy controls may also be offered during the sign-up process for a new online service or account. Always explore and understand privacy controls available to you on a given website before exploring.

Also, please remember to sign out of your accounts – especially if you use a shared device for accessing your email, social media or another service that requires login. Users at cyber cafes often forget to sign out from their accounts – whoever next uses that shared facility can easily get into your accounts, and even highjack them!

PROTECTING DIGITAL ASSETS

A few simple but important precautions can help protect your digital assets.

A password, also called a passcode, is a memorized secret used to confirm the identity of a user. In the digital context, it is a combination of letters, numbers or punctuation marks arranged in a specific manner.

Using secure passwords is an important step in protecting your digital assets from unauthorized access or hacking. A password need not be an actual word: a non-word may be harder to guess, which is a desirable property of passwords.

Here are a few basic tips for better password protection:

- Always pick strong passwords to secure your accounts. Use a long password made up of numbers, symbols and uppercase and lowercase letters.
- Try using a phrase that only you know as the password
- Avoid using obvious personal information such as your birthday, anniversary, address, city of birth, high school, and relatives and pets
- Use a unique password for each of your accounts: Reusing passwords for important accounts is risky. If someone gets your password for one account, they could access your email, address and even your bank accounts.
- Remember to setup your password recovery options if you forget a password
- Change your passwords regularly - the more often you change your password is better
- Allowing web browsers to remember your passwords may seem convenient but is a risky practice. If someone else enters your device, they can easily access all your accounts.

WHAT ARE DIGITAL ASSETS?

In the simplest terms, a digital asset is content that is stored digitally. That could mean images, photos, videos, files containing text, spreadsheets, or slide sets. Digital assets may be stored on a computer's hard drive, in a smartphone memory or online.

Digital assets also include your accounts for key digital services like email and social media.

USING TWO-STEP AUTHENTICATION

After setting up strong passwords, the next most important step is to enable two factor authentication (also known as two step verification or two step authentication).

It means that in addition to a password, you will need to provide a second piece of information to log in to your accounts -- usually a code that is sent to your registered mobile phone as a text message or SMS (and is valid only for a single use within a few minutes). All major social media platforms, as well as services like Google have now introduced two step authentication as a security option.

If a web service supports both text- and app-based two factor authentication, please select app-based. This is because SMS text messages are not encrypted, and could therefore be intercepted.

PASSWORDS ARE SECRETS!

Passwords are meant to be personal and confidential. They are not for sharing. And certainly not for display in any manner or form. Yet this is one of the most common mistakes many people and some organizations make – often to later regret. So please remember: a password can protect your digital assets only if you keep it secret!

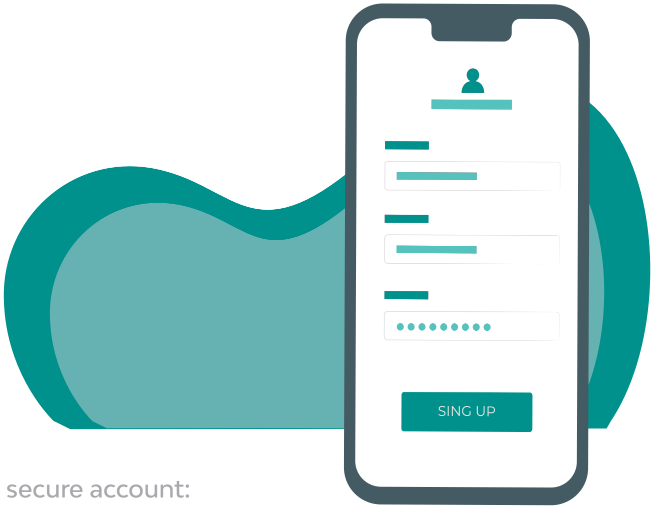
MOBILE PHONE SECURITY

Every mobile phone, GSM modem or device with a built-in phone/modem has a unique 15-digit IMEI (International Mobile Equipment Identity) number.

The IMEI was created because the SIM card number cannot be a permanent identifier of the device. (SIM Card is associated with the user and can be easily transferred from the phone to another phone.) Based on the IMEI number, you can check some information about the device, e.g. its brand and model.

The easiest way to check IMEI on any phone is to use the *#06# sequence. The IMEI number is useful when you would like to send the device for service to fill out warranty forms. Besides that, if you want to report a stolen or a lost phone at the police or network operator, you will need to know the IMEI number. After that you can ask your phone to be blocked, after which the device will be unusable, whether or not the SIM card is changed.

Please make sure you know your phone's IMEI number and have it written somewhere.



[1] Google has some useful advice on creating a strong password and a more secure account: https://support.google.com/accounts/answer/32040?hl=en

Here are a few basic tips for enhancing the security of your mobile phone:

- Set a strong pin number for activating the phone: use a six-digit code minimum.
- Download software updates regularly
- Get antivirus or anti-malware protection for your mobile devices.
- Download apps only from trusted platforms (e.g. Google play store and Apple app store)
- Control app permissions: Both Android and IOS systems have tools to make it easier to control exactly what each app on your devices can and cannot access. Limit the permissions so apps only have permissions to access data that it really needs to function. (Mypermissions.Com is a handy tool that allows you to check your permission settings across a multitude of apps, get reminders to clean your permissions with mobile-friendly apps, and get alerts when apps access your personal information so that you can remove it with a single click)
- Enable remote location and device-wiping: If your device is lost or stolen, tracking apps can tell you where your phone is. These apps also let you wipe sensitive information remotely.
- Disable Bluetooth when you are not using it: Bluetooth opens the door for vulnerabilities. Bluetooth attacks depend on exploiting the permission request/grant process that is the backbone of Bluetooth connectivity. The only way to completely prevent attackers from exploiting that is to turn off the Bluetooth function when not in use. Putting it into invisible or undetectable mode can still expose your device to Bluetooth attacks.

DIGITAL IDENTITY THEFT

Identity theft can happen both online and offline. It means the unauthorized collection of personal information and its subsequent use for criminal purposes such as to open credit cards and bank accounts, redirect mail or email, obtain a mobile phone connection, etc. The consequences can be very serious for the victim.

There are many ways in which an individual's identity can be stolen. People are vulnerable to this when using online services, where criminals can gain access to personal information through different ways.

Identity thieves have several ways of stealing personal information via electronic means. These include:

- Retrieving stored data from discarded electronic equipment such as PCs, mobile phones or USB memory sticks
- Stealing personal information using malware such as keystroke logging or spyware
- Hacking computer systems and databases to gain unauthorized access to large amounts of personal data
- Phishing, which means impersonating trusted organizations (such as a bank or a retailer) via email or SMS messages and prompting users to enter personal financial information
- Compromising weak login passwords (often through calculated guesswork) to gain access to a user's online accounts
- Using social networking sites to attain enough personal details to guess email passwords or impersonate the victim in other ways online
- Diverting victims' emails to attain personal information such as bank and credit card statements, or to prevent the victim from discovering that new accounts have been opened in his/her name

We cannot totally avoid the hazard of identity theft, but we can safeguard ourselves through awareness and constant vigilance. Here are a few tips offered by an online source:

- Beware of being redirected to a "middle-man" website when you think you are on a secure site, such as your bank's webpage. Check for suspicious URLs.
- Keep track of your credit card and banking statements to check for any suspicious transactions.
- Use only secure websites for financial transactions. If you enter credit card information online to make a purchase, you should see a lock in your browser's status bar, usually in the left corner. If you don't see the lock, don't enter your information.
- Don't answer emails or follow links in emails claiming to be from reputable institutions like your bank or university that ask for personal information. Contact the institution in question via phone or their website about these emails.
- Use common sense. If an offer sounds too good to be true ("Just enter your credit card number for a free trip to Paris!"), it is likely to be a scam!
- Don't send any personal information when using public WiFi.
- Look out for emails claiming to be from companies such as Norton Anti-Virus that prompt you to download something. Get in touch with the company independently (do not reply to the email itself) to check on the information.

[2] More information at: https://www.imei.info/
[3] Source: https://www.techopedia.com/definition/13637/identity-theft

CASE STUDIES

CASE STUDY 1: DATA DETOX KIT

It can be difficult to know where to start when it comes to reducing your data trail, becoming more digitally secure, or building a healthier relationship with technology. As our devices become more intertwined with our personal lives, it helps to find a balance.

The Data Detox Kit is a simple, accessible toolkit that walks you through the steps you can take towards a healthier online self. It takes a holistic approach, going through the different aspects of your digital life, from the amount of time you spend on your phone, to the apps that you use, to the passwords you set.

The Data Detox Kit has been produced by Tactical Tech, an international non-profit organization that engages with citizens and civil-society groups to explore and mitigate the impacts of technology on society.

Its printed version has been translated into Dutch, French, German, Indonesian, Norwegian, Polish, Portuguese, Spanish and Swedish. You can request a PDF copy at datadetox@tacticaltech.org, indicating the language you need, as well as your idea of how and where you'd like to use it.

Website: https://datadetoxkit.org/en/home

[4] Source: http://www.digitalresponsibility.org/how-to-avoid-online-identity-theft

CASE STUDY 2: THE DIGITAL FIRST AID KIT

The Digital First Aid Kit came about when a number of organizations working in the digital emergency field observed that once a person is targeted digitally, he or she often does not know what to do or where to turn for assistance. It was inspired by the belief that everyone has the ability to take preventative measures to avoid emergencies and responsive steps when they are in trouble.

The Digital First Aid Kit aims to provide preliminary support for people facing the most common types of digital threats. The Kit offers a set of self-diagnostic tools for human rights defenders, bloggers, activists and journalists facing attacks themselves, as well as providing guidelines for digital first responders to assist a person under threat.

The Kit begins with ways to establish secure communication when you or a contact are facing a digital threat and want to reach out for support. The Kit then moves on to sections on account hijacking, seizure of devices, malware infections and DDoS attacks.

These questions will guide you through a self-assessment or help a first responder better understand the challenges you are facing. It then lays out initial steps to understand and potentially fix the problems. The steps should also help you or a first responder to recognize when to request help from a specialist.

The Digital First Aid Kit gives you tools that can help you make a first assessment of what is happening and determine if you can mitigate the problem on your own. If at any moment you feel uncomfortable or unsure about implementing any of the solutions outlined here, ask for help from trained professionals, say its developers.

The self-diagnostic quality of the Kit should also enable journalists, bloggers, activists and human rights defenders to understand what is happening to their digital assets, to be able to determine more rapidly when they should reach out for help, what kind of help they need, and improve individual digital safety.

More: https://www.digitaldefenders.org/digitalfirstaid/

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- Digital security and cybersecurity is a shared responsibility of the user, and the provider of technology services. Do you agree? Discuss.
- Have you experienced a virus or malware problem and if so, what course of action did you or your organization take to resolve it?
- Have you activated encryption for any of your digital services? If so, describe your experience.
- In the event of a data or privacy breach, what can be done? Do you or your organization have a contingency plan?
- Do you know of any instance of digital identity theft? How did it happen and what recovery was possible?
- Do you use public Wi-Fi when away from your home and office? If so, what precautions do you take?

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- Cybersecurity is about systems and things; cyber safety is about people.
- Digital security and cybersecurity is a shared responsibility of the user, and the provider of technology services. Good digital security and cybersecurity requires user involvement, responsibility and vigilance.
- Strong passwords, two-step authentication, data encryption and regular data backups are among the precautionary measures that every user of digital services and the web should take. They are part of essential digital responsibility, also called good digital hygiene.
- There is plenty of free and helpful advice online about enhancing digital security and cybersecurity. However, the most important element in this process is you – the user!

FURTHER READING

Good Digital Hygiene: A guide to staying secure in cyberspace
Book by Ed Gelbstein (2013)
http://index-of.co.uk/IT-managment/good-digital-hygiene.pdf

Norton internet security advice
https://us.norton.com/internetsecurity

Google help centre (only for those with a Google account)
https://support.google.com/

Security in-a-Box, a guide to digital security for activists and human rights defenders
https://www.frontlinedefenders.org/en/digital-security-resources

Umbrella is digital and physical security for people at risk on your Android phone
https://secfirst.org/

Information security handbook for journalists
http://www.tcij.org/resources/handbooks/infosec

Electronic Frontier Foundation’s Surveillance Self Defence
https://ssd.eff.org/en

Tips on good digital hygiene
https://wiobyrne.com/digital-hygiene/

Digital security for activists, by the Electronic Intifada
https://electronicintifada.net/content/guide-online-security-activists/17536

●●●

MODULE 4

PROMOTING DIGITAL SAFETY

PROMOTING DIGITAL SAFETY

As noted earlier, cybersecurity is about systems and devices; cyber safety is about people who use them.

This module covers the basics of digital and cyber safety, i.e. the personal safety of human beings when they use digital technologies and web services.

Many people equate security with safety. But the two concepts are not the same. It is important to understand the difference.

A common approach is to secure digital devices, data and even digital identity. All this is necessary -- but not sufficient. Safety is addressed only when the needs and realities of human users are factored in.

To be safe can mean to be secure, but to be secure does not necessarily mean a person is safe. The ways we talk about safety and security are important as we think about the healthy digital ecosystem we hope to create.

To create a healthy digital ecosystem, we need to promote qualities like trust, good relationships and collaborations. We also need progressive laws and regulations as well as effective law enforcement.

Research that analyses and identifies key trends and recommends policy and regulatory responses provides the knowledge base for such action.

Collaborations can emerge from alliances between the tech industry, law enforcement agencies, civil society groups and individual users.

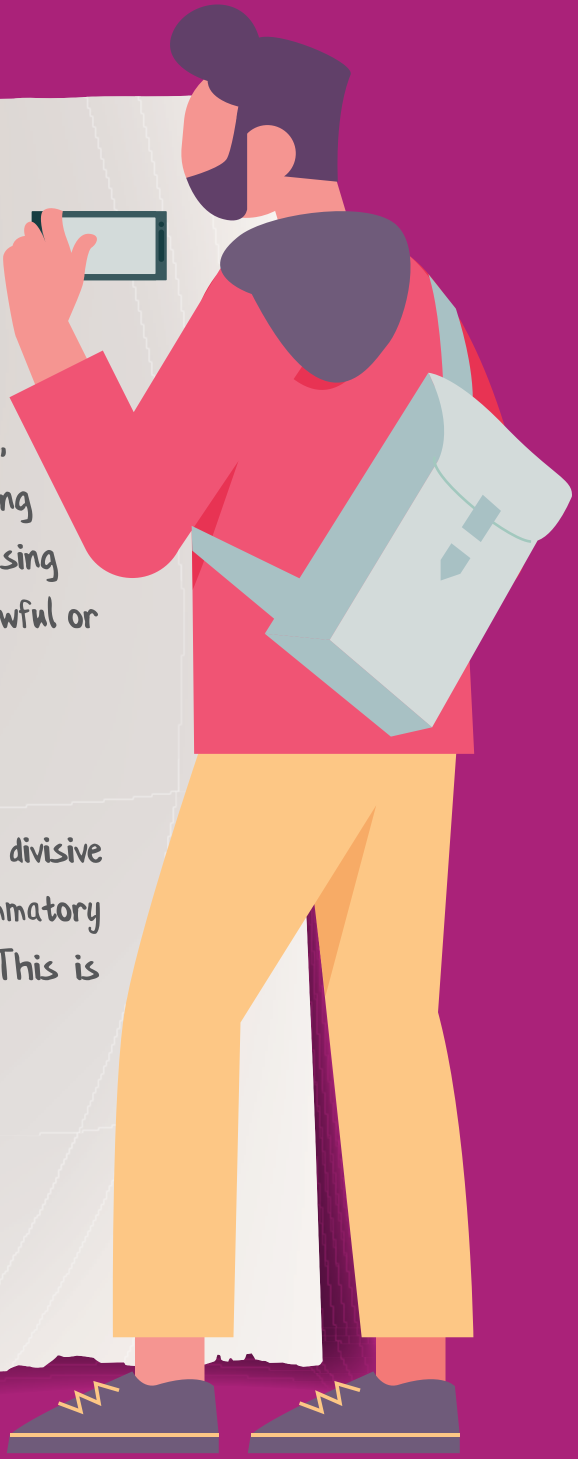
KEY TERMS

Cyberbullying: Cyberbullying is bullying that takes place over digital devices like mobile phones, computers, and tablets. It can occur through SMS and apps, or online in social media, forums or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting or sharing negative, harmful, false or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses into unlawful or criminal behaviour.

Source: https://www.stopbullying.gov/cyberbullying/what-is-it/index.html

Troll is a member of an internet community who posts offensive, divisive and controversial comments. Often, a troll will make obviously inflammatory statements that are meant to bait other users into reacting. This is called trolling.

Source: https://www.techopedia.com/definition/429/troll v



DIGITAL SAFETY AND HUMAN RIGHTS

We need to approach digital safety based on human rights: everyone, everywhere has a right to a safe and secure internet experience without any discrimination or harassment.

As mentioned in Module 1, the same human rights that people have offline must also be protected online.

The relevant human rights includes online aspects of the following: right to freedom of expression (which includes the right to information); right to privacy and data protection; rights of people with disabilities; and gender rights.

These rights are cross-cutting and interlinked. For example, the freedom of expression and information is related to access to the internet and net neutrality. Protection of minority rights is influenced by multilingualism and promotion of cultural diversity. Ensuring the protection of privacy is important in dealing with cybersecurity as well as cyber safety.

[1] Net neutrality is the principle that internet service providers (ISPs) must treat all internet communications equally, and not discriminate or charge differently based on user, content, website, platform, application, type of equipment or method of communication. More: https://www.eff.org/issues/net-neutrality

TECHNOLOGY-RELATED VIOLENCE AGAINST WOMEN

Digital safety is a concern for everyone who uses digital technologies. However, as women and children are disproportionately targeted online for harassment and cyber exploitation, their needs merit priority attention.

The Association for Progressive Communications (APC), a global network of civil society organizations, works to strengthen women's rights activists to use technology tools in their work. When it comes to violence against women, they highlight how that violence is increasingly linked to technology.

According to APC, the most common cases of technology-related violence against women are cyberstalking, sexual harassment, surveillance and the unauthorized manipulation of women's personal information including images and videos.

Even as these violations are rising, many women and girls who fall victim do not know what to do to stop the abuse, what they can report to whom, and what help they can expect.

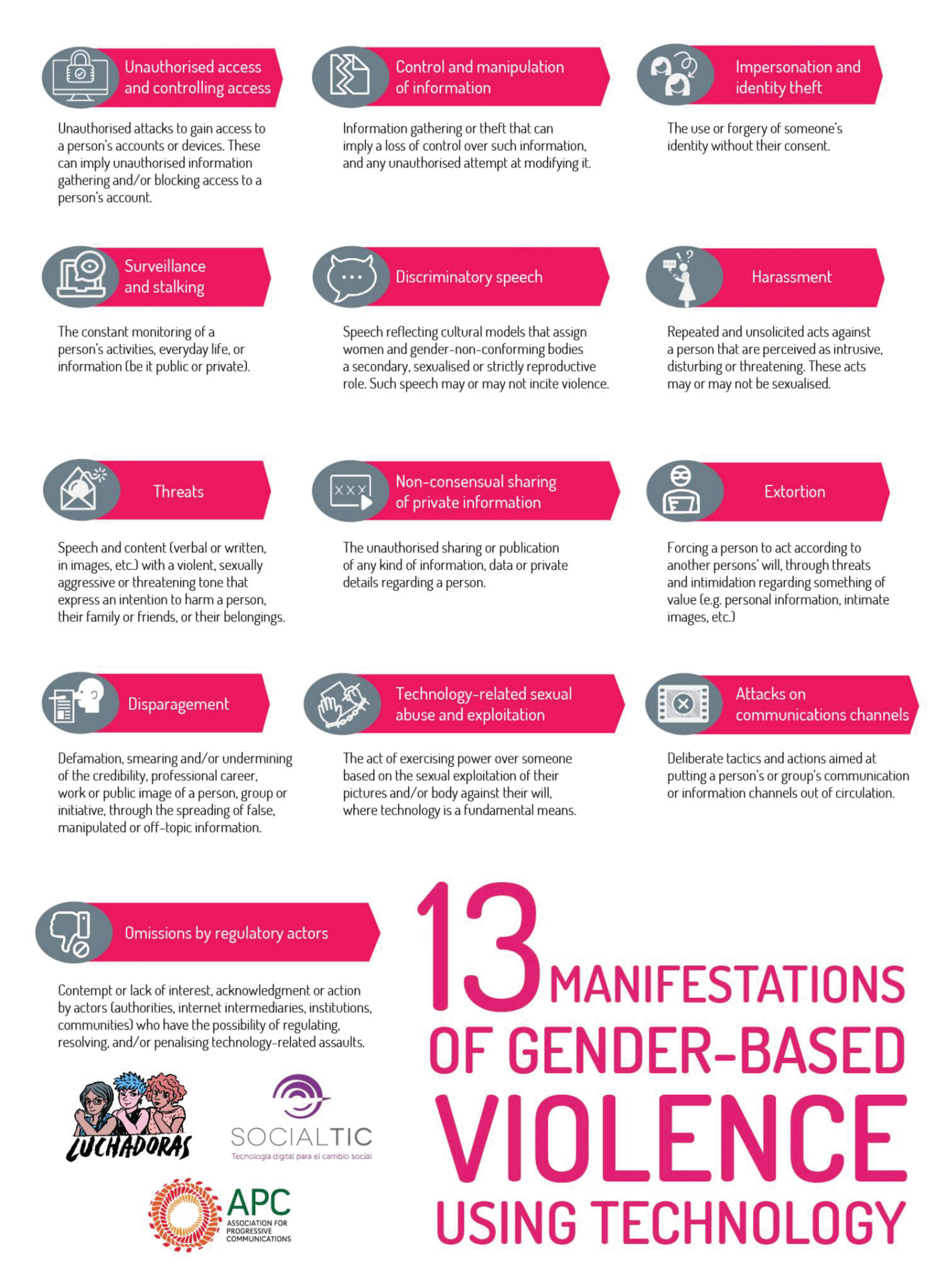
Many countries do not yet have policies, regulations or services to respond to these new forms of violence, or they are inadequate. Together with Mexican campaigners Luchadoras and SocialTic, APC has developed a longer list of 13 types of online gender-based violence.

"ONLINE VIOLENCE AGAINST WOMEN IS AN OVERT EXPRESSION OF THE GENDER DISCRIMINATION AND INEQUALITY THAT EXISTS OFFLINE. ONLINE, IT BECOMES AMPLIFIED."

JAC SM KEE, APC WOMEN'S RIGHTS PROGRAMME MANAGER

For a more detailed discussion on human rights online, see:
[2] https://dig.watch/baskets/human-rights
[3] https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology

https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology



13 MANIFESTATIONS OF GENDER-BASED VIOLENCE USING TECHNOLOGY

Unauthorised access and controlling access

Unauthorised attacks to gain access to a person's accounts or devices. These can imply unauthorised information gathering and/or blocking access to a person's account.

Control and manipulation of information

Information gathering or theft that can imply a loss of control over such information, and any unauthorised attempt at modifying it.

Impersonation and identity theft

The use or forgery of someone's identity without their consent.

Surveillance and stalking

The constant monitoring of a person's activities, everyday life, or information (be it public or private).

Discriminatory speech

Speech reflecting cultural models that assign women and gender-non-conforming bodies a secondary, sexualised or strictly reproductive role. Such speech may or may not incite violence.

Harassment

Repeated and unsolicited acts against a person that are perceived as intrusive, disturbing or threatening. These acts may or may not be sexualised.

Threats

Speech and content (verbal or written, in images, etc.) with a violent, sexually aggressive or threatening tone that express an intention to harm a person, their family or friends, or their belongings.

Non-consensual sharing of private information

The unauthorised sharing or publication of any kind of information, data or private details regarding a person.

Extortion

Forcing a person to act according to another persons' will, through threats and intimidation regarding something of value (e.g. personal information, intimate images, etc.)

Disparagement

Defamation, smearing and/or undermining of the credibility, professional career, work or public image of a person, group or initiative, through the spreading of false, manipulated or off-topic information.

Technology-related sexual abuse and exploitation

The act of exercising power over someone based on the sexual exploitation of their pictures and/or body against their will, where technology is a fundamental means.

Attacks on communications channels

Deliberate tactics and actions aimed at putting a person's or group's communication or information channels out of circulation.

Omissions by regulatory actors

Contempt or lack of interest, acknowledgment or action by actors (authorities, internet intermediaries, institutions, communities) who have the possibility of regulating, resolving, and/or penalising technology-related assaults.

LUCHADORAS
SOCIALTIC
Tecnología digital para el cambio social
APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

CYBER EXPLOITATION AND VIOLENCE

Cyber exploitation and violence (CEV) is the use of ICTs to bully, blackmail, harass, victimize, stigmatize, discriminate, coerce or in any way cause harm to a person's mental, physical or emotional well-being.

CEV can manifest itself in many ways, according to the Bakamoono.lk website managed by the Grassrooted Trust, a Lankan organization working on creating safe spaces for marginalized communities both online and in the real world.

- **Trolling** (in terms of the internet) is the deliberate act of someone making random unsolicited and/or controversial comments online – usually to provoke an emotional reaction from readers to engage in an argument.

- **Cyberstalking** is a criminal practice where an individual uses the internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging and any other online medium. Cyberstalking can also occur alongside offline stalking.

- **Identity theft** is the unauthorized collection of personal information and its subsequent misuse to open credit cards and bank accounts, redirect mail, obtain a mobile phone subscription, etc. Impersonating another person online or offline is a criminal activity.

- **Cyberbullying** is when someone bullies or harasses others on social media. Harmful bullying behaviour can include posting rumours, threats, sexual remarks, publishing a victim's personal information or use of racist or sexual insults (hate speech).

- **Revenge Porn** (also known as Girlfriend Porn, or Collecting and Exchanging Nudes, or Slut Shaming) involves pictures and videos of a sexual nature being shared online by former partners who have since fallen out and are now using such material – once exchanged in confidence - for public revenge.

There have been very few studies on CEV in the Sri Lankan context, even though anecdotal evidence suggests that the issues are very much present in society. A recent study conducted jointly by researchers from three advocacy groups -- the Centre for Policy Alternatives (CPA), Ghosha and Hashtag Generation – looked at how women are discussed on Facebook, the most popular social media platform in Sri Lanka with over 6 million monthly active users.

Their report includes findings from focus group discussions conducted with members of the Lesbian, Bisexual and Transgender (LGBT) community on their experiences relating to technology-based violence, as well as views gathered through interviews with female politicians and activists outside Colombo.

Researchers in this study monitored 52 Facebook accounts over a period of 6 months in English, Sinhala and Tamil. Apart from meme pages and public Facebook groups dedicated to specific special interests or hobbies, the pages monitored included those of public figures such as politicians and local celebrities. The study notes: "What emerged was a clear pattern of speech that was sexist, or objectified, harassed or otherwise targeted women and members of the LGBT community. The non-consensual dissemination of intimate photos and videos was another disturbing trend found in the lead-up to this study, with entire pages dedicated to such content, or alternatively linking to such content on third-party websites. The findings of this report indicate the normalisation of sexist commentary, escalating to and including violence against women and LGBT communities, both online and offline."

This study has highlighted the culture of sexism and misogyny that exists on Facebook which was common across Sinhala, Tamil and English languages. Researchers believe this is an extension of the casual sexism that already exists on Facebook and in Lankan culture in general. This is often packaged (and justified) as 'humour'. There were also instances where the page or poster seemingly defends women whilst, in fact, propagating violence against them.

The internet's anonymity is being exploited by many followers or commentators using fake identities, the researchers found – this makes it difficult to report such pages to Facebook administrators. The study also discovered that those involved have found ways to work around Facebook's community standards, using tactics such as posting only links, or placing text over images, or only liking posts without sharing them.

[4] https://groundviews.org/2019/06/27/opinions-btch-technology-based-violence-against-women-in-sri-lanka/

"OUR RESPONSE AS PARENTS, TEACHERS, AND CONCERNED ADULTS, CANNOT BE TO BAN THE USE OF SOCIAL MEDIA, OR THE USE OF HANDHELD ONLINE DEVICES. THE BENEFIT OF BEING ONLINE IN TERMS OF KNOWLEDGE GATHERING AND KNOWLEDGE SHARING IS IMMEASURABLE. THE ONLINE WORLD IS ANOTHER SPACE WHERE WE COMMUNICATE WITH EACH OTHER, WHERE WE BUILD RELATIONSHIPS. WE MUST BE CONSCIOUS OF RESPECT FOR SELF, RESPECT FOR THE OTHER, AND RESPECT FOR DIFFERENCE IN ALL OUR INTERACTIONS, BOTH ONLINE AND OFF IT." –

BAKAMOONO.LK

"IT IS INCREASINGLY POSSIBLE TO CHALLENGE THE FALSE DICHOTOMY OF ONLINE VS. OFFLINE VIOLENCE. TECHNOLOGY-RELATED VIOLENCE DOES NOT EXIST IN ISOLATION AND IS AN EXTENSION, AND OFTEN FORMS AN INTEGRAL PART OF, THE VIOLENCE EXPERIENCED BY WOMEN, GIRLS AND LGBT PEOPLE... TECHNOLOGY-RELATED VIOLENCE DOES NOT OCCUR ENTIRELY ON THE INTERNET – TEXT MESSAGES OR PHONE CALLS ALSO FALL INTO THE SPECTRUM. THE CONSEQUENCES, SUCH AS VIOLATIONS OF WOMEN'S RIGHT TO PRIVACY, EDUCATION, WORK AND HEALTH, DO NOT EXIST SOLELY ONLINE. THE SAME DISCRIMINATIONS, VIOLATIONS AND SURVEILLANCE FACED IN PUBLIC AND PRIVATE SPHERES ARE REPLICATED ONLINE AND IN SOME CASES, EXACERBATED." -

OPINIONS, B*TCH: TECHNOLOGY-BASED VIOLENCE AGAINST WOMEN IN SRI LANKA (CPA, Ghosha and Hashtag Generation, 2019)

SOCIAL MEDIA COMMUNITY STANDARDS

All key social media platforms have rules for their users. These are widely known as community standards. Everyone agrees to abide by these rules when starting an account.

For example, the world's largest social media network Facebook had 2.38 billion monthly active users as of 31 March 2019. These users generate or react to billions of items of content every day and night. For the most part this global chatter is harmless. But not everyone plays by the rules. Facebook's Community Standards outline what is allowed or not on their platform. See: https://www.facebook.com/communitystandards/

"The goal of our Community Standards is to encourage expression and create a safe environment. We base our policies on input from our community and from experts in fields such as technology and public safety," says its introduction.

Facebook says its rules are built around three pillars: Safety (removing content that harms others), Voice (the ability for users to express diverse views and ideas), and Equity (applying the same standards to all users).

The rules don't allow content that encourages violence or criminal behaviour including terrorist and hate groups, human trafficking and organized crime. It also forbids trading in "regulated goods" like drugs or firearms. Facebook will remove posts that encourage self-harm or suicide, and those involving sexual exploitation (of children or adults).

Additionally, the rules list content deemed objectionable, which includes graphic violence and hate speech, defined as "a direct attack on people based on what we call protected characteristics — race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, and serious disability or disease."

Rule breakers face consequences. First breach could draw a warning, and repeated violations can lead to restrictions in the user's ability to post. Serial offenders will see their profile (account) disabled. "We may also notify law enforcement when we believe that there is a genuine risk of physical harm or a direct threat to public safety," say the rules.

Other platforms like Instagram, YouTube and Twitter also have their own rules. We encourage you to read and understand these rules which are attempts to self-regulate social media.

HOW TO REACT TO CYBER EXPLOITATION AND VIOLENCE

Raising awareness and promoting user level precautions are the first steps.

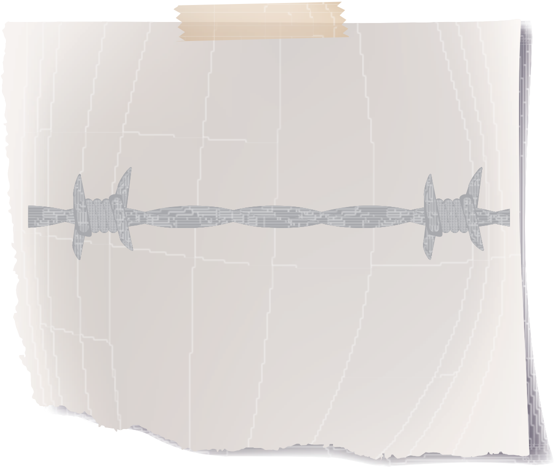
There are many helpful online resources as well as campaigns and self-help groups. Here are two international examples:

- **Take Back The Tech!** is an initiative by APC. It is a call to everyone, especially women and girls, to take control of technology to end violence against women. It's a global, collaborative campaign project that highlights the problem of tech-related violence against women, together with research and solutions from different parts of the world. The campaign offers safety roadmaps and information and provides an avenue for taking action. Take Back the Tech! leads several campaigns at various points in the year, but thier biggest annual campaign takes place during 16 Days of Activism Against Gender-Based Violence (25 November to 10 December). https://www.takebackthetech.net/

- **Safer Internet Day (SID)** is an international day of awareness for the risks involved in using the internet. Originally created in 2004 by the European Union, it is observed on the second day of the second week of February each year. SID has become a landmark event in the online safety calendar. It is now celebrated in approximately 140 countries worldwide. From cyberbullying to social networking, each year Safer Internet Day aims to raise awareness of emerging online issues and chooses a topic reflecting current concerns. https://www.saferinternetday.org/

In Sri Lanka, several civil society and advocacy groups offer information, advice or support that are related to digital safety and/or digital responsibility.

- **The Grassrooted Trust** was set up to provide a safe space for marginalized communities, online and in the real world. http://www.grassrooted.net/
- **Bakamoono.lk** is a trilingual website managed by the Grassrooted Trust and its partners. Its work is focused on issues related to sex and relationships and includes information on consent, gender, cyber exploitation and violence. http://www.bakamoono.lk/en
- **Women in Need (WIN)** is dedicated to addressing issues of gender based violence faced by women and girls in Sri Lanka. It has a team of lawyers and counsellors. https://www.winsl.net/
- **Shilpa Sayura** Foundation promotes responsible ICT use by youth. It implements the 'Respect Girls on Internet', a voluntary initiative to address cyber harassment of girls on social networks (see also Case Study 1 in this module) http://www.shilpasayura.org



[5] http://counterpoint.lk/violence-is-violence-offline-or-online/

HOW TO REPORT CASES OF CYBER EXPLOITATION AND VIOLENCE

Three state institutions are involved in the official responses to cyber harassment:

- National Child Protection Authority (NCPA) leads the response for victims and perpetrators under 18.

- Cyber Crimes Division of the Police Criminal Investigation Department (CID) handles the matter if victims are over 18.

- Sri Lanka Computer Emergency and Readiness Team (SL-CERT) also records complaints they receive, and refers to both the CID Cyber Crimes and NCPA response mechanisms.

The NCPA is also working with policy makers to review and strengthen our existing laws for responding to all forms of child abuse, including CEV.

If a picture or video of you, or someone you know is online, e.g. on a website, inform Sri Lanka CERT on 011 2 691 692 immediately. If you do not receive the support you need and/or expected, get in touch with Women in Need on 011 471 85 85 to report the incident.

If the victim is over 18, you may also contact the CID Cyber Crime Unit directly on 011 232 6979 and email details of the incident to BOTH <dir.cid@police.lk> and <telligp@police.lk>

if the victim is under 18, approach the National Child Protection Authority on their hotline 1929 or visit their website: http://www.childprotection.gov.lk/

Here are some tips shared by the Grassrooted Trust on its website with regard to preserving evidence and information.

- If you are being blackmailed, ensure that any communications with the perpetrator are not deleted regardless of the platform that it is on. The police may require you hand in your phone to confirm the evidence first hand, ensure it is not doctored, etc. This could include messages, call logs, etc.
- We recommend for your records and information you take and store screenshots as well, as with some platforms like Instagram, Direct Messages can be unsent. When you make a complaint to the police speak to your lawyer or the person who accompanies you about asking if the police can take the screenshots on their computer or to certify the validity of the screenshots taken.
- If a phone is being handed over to the Police, you should have saved screenshots of all evidence. Ideally, you should create a list of all related material that can be found on the phone and give a copy of it along with the phone so that there is a clear acknowledgment of what was given.
- Keep a record of everything that has happened, for example if threatening phone calls/texts were received over the period of time, you should keep a written note of dates/times or approximate date/times and nature of the call/text. Keeping a chronological account is helpful when making a police complaint, will help them remember the order of events, and be clearer and more consistent when you are giving evidence or making a complaint.

[6] http://www.bakamoono.lk/en/article/2600/how-to-report-cases-of-cyber-exploitation-and-violence

LEGAL PROTECTION AGAINST CYBER HARASSMENT

Up to mid-2019, Sri Lanka did not have specific laws that criminalize cyber harassment.

However, some sections of the Penal Code could be used to address some aspects of it:

- Section 345 deals with sexual harassment (defining it as the use of words or actions to cause annoyance or harassment to a person)
- Section 372 deals with extortion (defining it as the intentional act of putting another person in fear of injury, inducing a person to deliver property or valuable security)
- Section 483 addresses criminal intimidation or threatening a person to act or omit an action in order to avoid some sort of punishment.

Of these, sections 372 and 483 can be used to tackle blackmail over the sharing of personal photos or videos captured using digital media and/or stored online.

Under the Obscene Publications Act (of 1927 and later amendments), the sharing personal, intimate images without consent, or sharing of images which have been explicitly altered using editing software, can be challenged. Section 2 of this Act makes it offences to possess, distribute or publicly exhibit of "obscene photographs".

In the Payment Devices Frauds Act (No 30 of 2006) section 3 (r) makes it an offence to obtain money or goods through a payment device with intent to defraud -- this can be used to tackle blackmail.

Section 7 of the Computer Crimes Act No 24 of 2007 makes it an offense for people to obtain information from a computer or a storage medium of a computer without permission. It also criminalizes downloading, uploading or making copies of such illegally acquired content.

DESPITE THESE LEGAL PROVISIONS, IT IS NOT EASY FOR VICTIMS TO ACCESS JUSTICE FOR CRIMES COMMITTED AGAINST THEM ONLINE. MOST VICTIMS DO NOT PURSUE LEGAL ACTION DUE TO FLAWS IN THE SYSTEM OF REPORTING ONLINE VIOLENCE TO AUTHORITIES. IN ADDITION, NOT ALL SURVIVORS MIGHT BE ABLE TO AFFORD LAWYERS TO SUPPORT THEMSELVES.

CASE STUDIES

CASE STUDY 1: RESPECT GIRLS ON INTERNET

A few years ago, Poornima Meegammana was busy preparing for her GCE Advanced Level (university entrance) exam. The day before the exam was to start, she received some 'really nasty' messages -- seemingly from a trusted male friend's Facebook account.

"I was stunned by these messages and didn't know what to make of them. I least expected such a thing from this friend, and I was psychologically very affected. It was only later that I found out that someone else – also known to both of us – had accessed my friend's account without authorisation and sent those messages."

Poornima coped with the trauma with the understanding and support from her family and close friends. But she realised that the phenomenon was widespread and how girls and women were especially being targeted.

Turning her bitter experience into a positive action, she founded 'Respect Girls on Internet', a voluntary initiative to address cyber harassment of girls on social networks, including extreme cases of self-harm. The effort is anchored within the non-profit Shilpa Sayura Foundation.

Poornima says many teenagers typically start using the internet without any knowledge about cyber safety or privacy. Young persons who experience cyber bullying tend to withdraw from social life and digital activities while the physical and/or psychological effects impact their studies or work.

“There are laws and procedures for protection, but there is a lack of awareness, advice and resources available – especially in local languages -- for victims to seek justice. Respect Girls project creates digital content to raise awareness about the problem, advocate for safe and respectful online discourse and promote empathy. One of the project’s key outputs is a Cyber Privacy e-Handbook for teenagers new online, as well as for teachers and parents.

Respect Girls also acts as a network of youth for preventing cyber harassment, and as a support group for victims.

In 2017, the Internet Society selected Poornima for a 25Under25 Award recognising young people around the world who are taking action and using the Internet as a force for good.

More: http://respect-girls-on-internet.blogspot.com/
https://www.internetsociety.org/25th/25-under-25/awardees
https://www.bbc.com/sinhala/sri-lanka-41218095

CASE STUDY 2: REVENGE PORN IN SRI LANKA

‘Revenge porn’ is a commonly used term for the non-consensual distribution or publication of intimate images or videos online. This practice has been growing in Sri Lanka, even though most victims choose not to report or seek legal help.

Feminist activist and researcher Sharanya Sekaram from the Grassrooted Trust describes one of the many revenge porn networks her organization had unearthed in their research: a WhatsApp group, and to be a part of the group each individual had to submit five explicit pictures of nude females.

“The question is: what has made these boys come to consider a naked picture as some form of currency? How do they think they have ownership over these?” she asks.

She relates another incident in which a girl had been asked by an ex-boyfriend to “get on video call” and “please” him, or risk having her intimate pictures circulated. When the girl refused, the perpetrator had responded saying that she had better consent if she values her life, because once her pictures are released, her life would be ruined.

“This shows that the perpetrators are often perfectly aware of the repercussions their victims will face if these explicit images or videos are ever released. They know how our society works and where the blame will invariably lie. They know what damage they can do.”

Sharanya believes that the problem is one rooted in culture, patriarchal notions and societal attitudes rather than technology. She says revenge porn should be viewed through the same lens as intimate partner violence and gender-based violence.

“People view online violence as an isolated problem, but they haven’t been connecting the dots,” she says. She adds that existing laws in Sri Lanka can be invoked when reporting such crimes, e.g. Section II of the Obscene Publications Act deals with the distribution, exhibition, and possession of obscene images.

However, public institutions with the mandate to act are ineffective, and victims are often treated with insensitivity – discouraging those who seek justice. The widespread culture of victim-shaming, which blames the victim rather than the perpetrator, also makes victims reluctant to come forward.

Adapted from: https://roar.media/english/life/in-the-know/cyber-exploitation-and-violence-the-darker-side-of-cyberspace/

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- How much can a user take precautions to guard herself against cyber harassment, exploitation and online violence? What user level actions are possible and practicable?

- “Online violence against women is an overt expression of the gender discrimination and inequality that exists offline.” Do you agree or disagree? Discuss.

- Digital and cyber safety are major concerns for children and women, but other marginalized groups are also vulnerable. Who or what are these groups? In what ways are they targeted online?

- Consensual sharing of intimate photos and videos between two persons in a relationship has become easier with smartphones and the web. Is this an inherently unsafe practice? What precautions are possible and advisable? Discuss.

- Don’t feed the trolls! As they thrive on attention and engagement, the best way to discourage trolls is to ignore them. But it doesn’t always work, so what other actions can be taken?

- The internet's anonymity is being exploited by those who engage in cyber harassment as they use fake identities. Should everyone be compelled to use online services only under their real identity? What implications can such a requirement have for vulnerable groups?

- Recent research found a culture of sexism and misogyny that exists on Lankan pages of Facebook which was common across all three languages. Is this a reflection of offline society? Is Facebook a mirror of our society?

- Have you reported about any problematic content to a social media platform like Facebook? If so, what was your experience?

- What do you think of community standards of social media platforms: are they adequate? Is there proper monitoring by the platforms? What more can be done?

- Why is it so difficult for victims to access justice for crimes committed against them online? How can law enforcement and justice process be more supportive and sensitive?

- Does Sri Lanka need new laws to strengthen digital and cyber safety? Or is it more a case of properly enforcing existing laws and increasing proactive action to tackle rising levels of cyber exploitation? Discuss.

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- To create healthy digital ecosystem, we need to promote qualities like trust, goodwill, good relationships and collaborations. We also need progressive laws, regulations and effective law enforcement.

- Internet and digital safety are concerns for everyone who uses these technologies. Cyber exploitation and violence threaten this safety.

- Preventing technology-related violence against women is an important component in ending violence against women in general: it contributes to creating a safe and secure environment for women and girls in every sphere of life.

- Facebook and other social media platforms, as they are used in Sri Lanka, are a reflection of disparities and inequalities that exist in society. For example: the culture of sexism and misogyny.

- All major social media platforms have their own rules, known as community standards. However, violators keep finding ways to get around these rules. Stronger vigilance and action are needed by both platforms and the user community.

- Victims of cyber exploitation and violence find it hard to access legal relief or justice. Most victims do not pursue legal action due to flaws in the system of reporting online violence to authorities.

- In this situation, it is various self-help groups and civil society organizations that offer advice, guidance and support.

FURTHER READING

Facebook Community Standards
https://www.facebook.com/communitystandards/

YouTube policies
https://www.youtube.com/yt/about/policies/

Twitter Rules
https://help.twitter.com/en/rules-and-policies/twitter-rules

Instagram Community Guidelines
https://help.instagram.com/477434105621119

Beyond the Report Button: Tackling Cyber-Violence in Sri Lanka.
A detailed discussion by Amalini De Sayrah, published on Bakamoono.lk
http://www.bakamoono.lk/en/article/2136/beyond-the-report-button-tackling-cyber-violence-in-sri-lanka

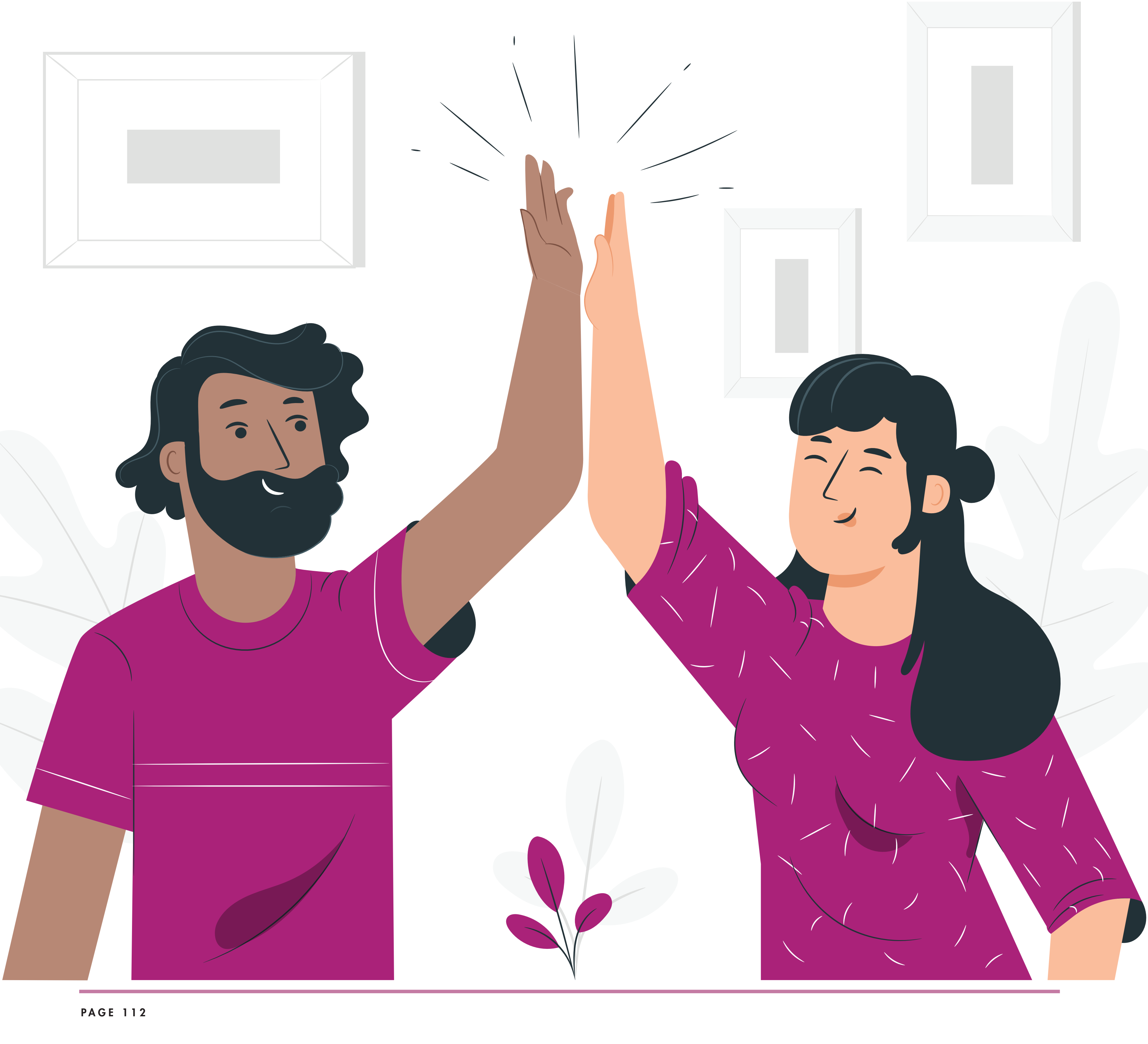
OPINIONS, B*TCH: Technology-based Violence Against Women in Sri Lanka
Centre for Policy Alternatives, Ghosha and Hashtag Generation, 2019
https://groundviews.org/2019/06/27/opinions-btch-technology-based-violence-against-women-in-sri-lanka/

Cyber-Exploitation and Violence: The Darker Side of Cyberspace.
Article by Radhia Rameez on Roar Media, April 2018
https://roar.media/english/life/in-the-know/cyber-exploitation-and-violence-the-darker-side-of-cyberspace/

Children's Rights and the Internet: From Guidelines to Practice. Unicef, 2016
https://www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf

Take Back the Tech! A call to take control of technology to end violence against women
https://www.takebackthetech.net/

Online gender-based violence: A submission from the Association for Progressive Communications to the UN Special Rapporteur on violence against women, its causes and consequences, November 2017
https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV.pdf



MODULE 5

NURTURING DIGITAL WELL-BEING

MODULE 5

NURTURING DIGITAL WELL-BEING

Today we use digital tools and services for work, study and leisure. We are spending more and more time online and interacting with these technologies. Such regular use over a long period of time can have impacts on our physical and mental health as well as on our social lives.

Digital wellbeing is a relatively new area that focuses on how our physical and psychological health can be affected by the regular use of digital technologies and services – and what we can do to maintain a healthy balance.

In this section, we explore what is currently known of such impacts, and also summarize advice on basic precautions and good practices.

Please note that this section does not cover what is known as 'digital health' or e-health, which is a specialized area where digital technologies are used for delivering healthcare services.

KEY TERMS

Digital wellness: A way of life, while using technology, that promotes optimal health and well-being in which body, mind, and spirit are integrated by the individual to live more fully within the human, natural, and digital communities. Ideally, it is the optimum state of health that each individual using digital technology is capable of achieving.

Digital well-being is a term used by health professionals, researchers and device manufacturers to describe the concept that when humans interact with technology, the experience should support mental and/or physical health in a measurable way.

Digital detox refers to a state when a person quits or suspends use of digital equipment and devices to use that time for social interactions and other activities. It enables that person to relieve stress and anxiety arising from intense use of digital devices like smartphones

PHYSICAL IMPACTS

It is no longer an option to discard the digital tools and services that have become integral to our lives. However, we can better manage the ways in which we use them, to minimize health impacts to our bodies and minds.

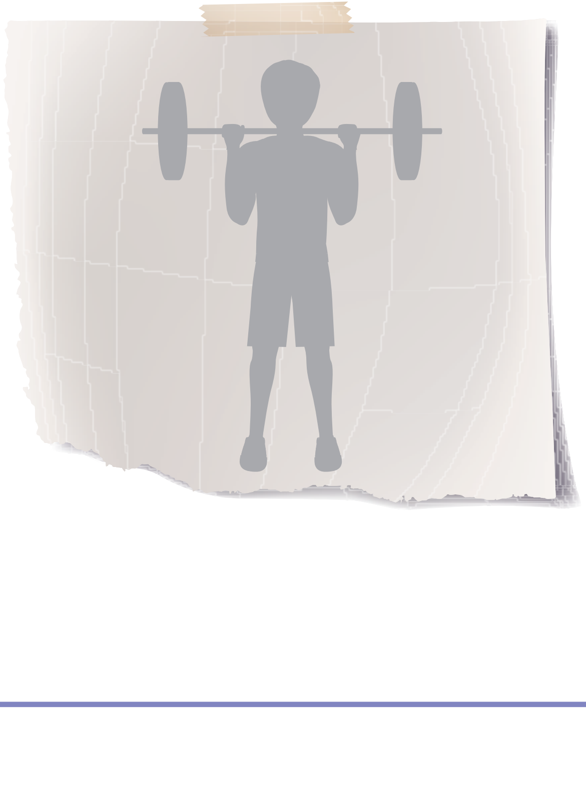
Spending several hours of each day looking at a digital screen, especially if the user is seated, can lead to long term health issues. Here are the key impacts on the body as currently known:

- **Eye strain**: Computer Vision Syndrome (CVS) is a complex of eye and vision problems related to the activities which stress the near vision and which are experienced during the use of computers. Symptoms can include eyestrain, blurred vision and dry eyes. (In addition to computer use, other factors can also contribute to eye and vision disorders in an office environment – these include air conditioners, ventilation fans, static build up, airborne paper dust and contaminants.)
- **Neck strain**: When you bend your head down to look at a computer screen, it exerts unnecessary strain on the neck muscles that can lead to muscle pains and even tension headaches. Laptop users have especially poor posture for the neck, as they tend to hunch down to look at screens. Holding a mobile phone between the neck and shoulder (as some people do, to free their hands) also puts the neck in an unhealthy position. Even texting involves a lot of hanging the head over your phone.
- **Too much sitting**: Many who use computers on a daily basis spend hours being seated at their work stations, and such sedentary lifestyle can lead to long-term health impacts including obesity, diabetes, heart attacks, high cholesterol and high blood pressure. Even if such persons take regular exercises, being seated for long can still be a health concern.

- **Hearing problems**: If you wear headphones regularly and for long periods of time for telephone conversations and/or for listening to music, it can lead to hearing problems and tinnitus (ringing in the ears).

- **Disrupted sleeping patterns**: Excessive use of digital devices can lead to poor quality sleep as well as reduced hours of sleep – both of which can have multiple health effects.

- **Repetitive Strain Injury**: The computer has made it possible for users to work all day at a keyboard without varying their pattern of movement significantly. This can lead to Repetitive Strain Injury (RSI), which can involve damage to muscles, tendons and nerves of the neck, shoulder, forearm and hand. These can cause pain, weakness, numbness or impairment of motor control. The three primary risk factors are poor posture, poor technique and overuse.



"SO, WE SHOULD LOVE OUR TECHNOLOGY, IT'S AMAZING HOW GOOD IT IS. THE PROBLEM WITH TECHNOLOGY IS NOT THAT IT'S BAD, IT'S THAT IT'S SO GOOD. SO WE LOVE IT, BUT MAYBE WE LOVE IT TOO MUCH. WE LOVE IT SO MUCH, WE DON'T ALWAYS REALIZE THE SACRIFICES WE ARE MAKING FOR THE SAKE OF OUR TECHNOLOGY. WE MAKE SACRIFICES IN PHYSICAL MOVEMENT. WE MAKE SACRIFICES IN OUR RELATIONSHIPS. WE MAKE SACRIFICES IN OUR ATTENTION, IN OUR TIME, IN OUR SLEEP, IN OUR CONNECTION TO NATURE. AND WE'RE MAKING ALL OF THESE SACRIFICES TODAY, FOR TECHNOLOGY THAT DIDN'T EXIST 20 YEARS AGO..."

JEREMY MCCARTHY, FROM A 2017 TALK AT THE
GLOBAL WELLNESS INSTITUTE

http://psychologyofwellbeing.com/201712/digital-wellness-wellness-in-the-age-of-technology.html

PSYCHOLOGICAL IMPACTS

Prolonged use of digital tools and services can affect our minds and moods too.

A number of specific conditions have already arisen as a result of the amount of time we are spending on digital devices: gaming addiction, which the World Health Organisation (WHO) recently listed as a mental health condition; the fear and anxiety of being away from mobile phones, officially called ‘nomophobia’; and behavioural addictions such as internet and social media addiction.

A 2012 study by the Pew Research Center’s Internet and American Life Project noted how “Millennials will benefit and suffer due to their hyperconnected lives.” Many experts and other stakeholders interviewed for this study generally agreed that those who best capitalize on new technologies will be able to access and sift through large amounts of information quickly. At the same time, ICTs can make users impatient, subject to frequent distraction, and desperate for constant entertainment.

Here are a few ways in which regular use of digital tools can impact our psychological and emotional health.

- **iDisorder:** Medical research is still underway about the long-term effects of digital technologies. Some experts have already cautioned about what they call “iDisorder” -- where users show signs and symptoms of a psychiatric disorder such as Obsessive Compulsive Disorder (OCD), narcissism, or Attention-deficit/hyperactivity disorder (ADHD), which are manifested through the use or overuse of technology. Symptoms include an obsessive need to check for text messages, a desperate desire to constantly update Facebook status, or a near-addiction to smartphone games.

- **Instant gratification:** Rising expectations of instant gratification is another concern. When we post a Facebook status, a tweet or an Instagram photo, it feeds on and reinforces our need for instant approving feedback. Becoming too used to such instant gratification in the virtual world can lead to poor choices and major frustrations in the physical world.

- **Narcissism:** Social media can help boost some users' self-esteem, but it can also encourage and provide an outlet for a me-centered mentality. It could even lead to narcissistic personality disorder, a mental condition in which people have an inflated sense of their own importance, a deep need for excessive attention and admiration, troubled relationships, and a lack of empathy for others.
- **Moods disorders:** Research has found that there is a link between social media use and mood disorders like anxiety and depression, but researchers also acknowledge that the relationship is complex. More research is needed before conclusions can be drawn.

[1] Details at: https://web.eecs.umich.edu/~cscott/rsi.html

ACTIONS TO MINIMIZE HEALTH IMPACTS

As we said earlier, we cannot avoid using digital technologies, but we can take steps to minimize the adverse health impacts from prolonged use.

Here are a few among many practical suggestions offered by health specialists:

- Place your computer in a location with adequate lighting and minimal glare, about 20 to 30 inches (50 cm to 76 cm) away from your eyes. Also, watch out for air sources near your desk that can dry out your eyes.

- Computer users should take measures to reduce glare on their screen. Ergonomic measures which can reduce glare include placing computer screens at a 90 degree angle to windows (they should never be placed directly in front of or behind a window) and to the side, rather than directly below light sources.

- Eye care is particularly important when looking at screens for a long time. Don’t forget to blink! We tend to blink less frequently than normal when using a computer.

- Take a 20-20-20 break for the eyes, i.e. staring at something at least 20 feet away for 20 seconds every 20 minutes. As an added bonus, staring into the middle distance can be a much-needed break for a tech-addled mind.

- If you can afford it, invest in ergonomically designed furniture that will give you better posture while seated and working. A better-placed desk chair or better lighting can make a big difference on your physical and emotional well-being.

- Don't take your smartphone or any other gadget to bed with you, or even keep it close. To avoid disrupting your sleep rhythms, turn off all your screens an hour or two before you go to bed and give your eyes a rest.

- Use a lower back support in your work chair to guide yourself into a healthier posture.

- To avoid constantly looking down, raise your laptop to eye level by placing something under it. You will need to use an external keyboard to type comfortably with your laptop in this position, but the benefits for your neck will be worth it.

- Do some exercises. While you're studying or working, take short breaks to do some simple movements like shoulder rolls. You may be hunching your shoulders up as you work at the computer without even realizing it. In your free time, try some training exercises to strengthen your neck muscles.

- Instead of multi-tasking with multiple forms of technology and media, try to concentrate on one at a time. Try disciplining yourself to devote an uninterrupted twenty minutes to each task, be it answering email or working on a writing assignment or listening to a podcast.

- Begin paying attention to how many forms of media you are using at once and ask yourself what your goal is. Simple awareness can help curb tech binges.

- Set a timer on your computer to go off every fifteen or twenty minutes to remind yourself to get back on task if you have strayed.

[2] https://www.pewinternet.org/2012/02/29/millennials-will-benefit-and-suffer-due-to-their-hyperconnected-lives/

PREVENTING RSI

The best way to prevent damage performed by repetitive actions is to stop doing the action!

Ensure you are not typing for long periods of time without a break. If you tend to do that without realising it, set a timer to alert you to take a break.

Correct posture is a crucial step to helping prevent RSI. The best is sitting with your back straight and fully supported, monitor at eye level, with your keyboard at around elbow height. If you catch yourself slouching, be sure to correct your posture before continuing.

Other advice includes: using a wrist pad, using a hand exercise during breaks, switching to a trackball mouse, and using an ergonomically designed keyboard.

More: https://www.webopedia.com/DidYouKnow/Internet/Web_vs_Internet.asp

HOW TO MANAGE DIGITAL HABITS

Technology has become so pervasive today that it can be hard to put down our smartphone or turn off our laptop. However, spending too much time with digital devices can be harmful to our health as well as social relationships.

Smartphone is the most widely used digital device in the world today. Most people use smartphones for daily functions like work emails, navigating and staying connected with family and friends. There are, of course, hundreds more apps with various uses.

Not everyone can voluntarily have a digital detox – that is, a period when a person stays away from using any digital or electronic device. A digital detox is done mainly to avoid being addicted or obsessed with digital devices and mentally relaxed by taking some time to enjoy the physical or real world.

Even without a digital detox, it is still possible to monitor and regulate how much we use our devices, especially smartphones. Consider these steps:

- Take regular breaks from screen use. A break can be as small as stepping away from your desk to take a short walk across the room, or as large as observing a 'technology blackout' for an entire day each week. Try cutting down on the number of posts or status updates you make each day. Ask yourself whether you are posting for narcissistic reasons, or with the goal of making true connections.

- Both Android and iOS (Apple) devices have recently introduced options to track the total screen time we use each day or week. These settings also allow us to define upper limits of screen time. There are also free apps that allow us to track our digital use patterns.

- We can also set our own boundaries for smartphone free spaces and times. For instance, try making a pact with yourself to put away phones during meals, family car rides, or an hour each evening.

- The blue light from digital device screens can disturb our sleep. Try not to look at any digital screen at least 30 minutes before going to sleep. Scientists also advise that we should not be looking at a digital screen immediately after we wake up.

Here are seven more good habits recommended by Techlicious website:

- Don't charge smartphones in your bedroom.

- Turn off all notifications — except for those from people. A good rule of thumb is to turn off all notifications except those that enable direct communication with people — in other words, block all apps and games from pushing alerts, including Twitter and Facebook

- Keep your home screen minimal: Remove all icons from your home screen except for the bare minimum of functional apps. This might include your maps, ride-hailing, camera and messaging apps.

- Turn your phone black-and-white (iOS and some Android phones only): colorful icons and app interfaces are tantamount to little rewards for the brain, positively reinforcing the action of checking our phones. They suggest turning your phone display to grayscale to help reduce unnecessary phone-checking.

- Set a schedule for when you read and respond to emails. Depending on how much your work requires you to be in constant contact, restricting when you check email could actually enhance your productivity.

- Use social media just enough: As with email, set times when you can check social media so that when you do, you are intentionally using the app, rather than mindlessly or compulsively scrolling.

- Restrict phone use around people: “Phubbing” is the practice of snubbing others in favor of our mobile phones, which is a bad habit. Studies show that once phubbed, someone is more likely to turn to their own phone, further reducing direct communication. So next time you are talking with someone in person, try keeping your phone out of sight and its notifications turned off

[3] https://www.techlicious.com/tip/how-to-build-better-digital-habits/

CASE STUDIES

CASE STUDY 1: TIME WELL SPENT MOVEMENT

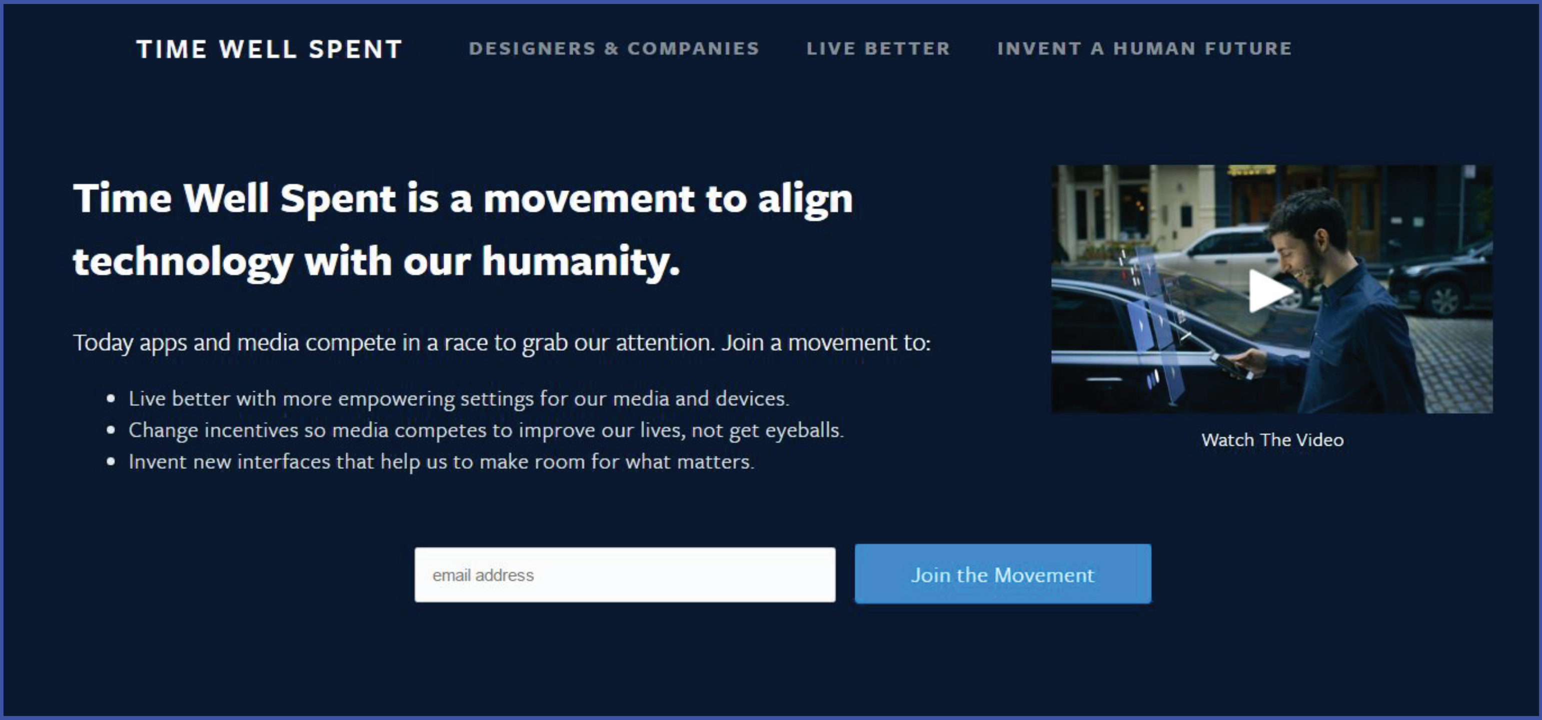
Tristan Harris was working as a product manager at Google in 2012 and, over time, he became increasingly disillusioned with the demands of digital technologies. He noticed every buzz of his phone was a distraction, and every Inbox notification took him away from his work and affected his concentration.

He soon realized that these were symptoms of the large-scale attention-grabbing business models promoted by his company and other tech companies providing digital services. He created a presentation called “A Call to Minimize Distraction & Respect Users’ Attention”, which went viral within Google, reaching thousands of employees. But nothing much happened.

So in 2016, Harris left Google to start a non-profit entity that was initially called ‘Time Well Spent’ (which has since been rebranded as the Centre for Humane Technology). It is committed to solving to the problems of the “attention economy.” Over two years, he has catalyzed a growing movement of cross-disciplinary leaders in technology, humanity, mindfulness, philosophy, and education.

Using mass media and social media, and through public talks (including TED talks), Harris has drawn attention to the fact that we spend too much time on our phones, and on social media. His solutions are simple: Turn your screen to grayscale (instead of colourful icons of various apps). Switch on the phone’s ”do not disturb” mode at night. When if go on a walk or run, leave your phone at home.

Time Well Spent movement’s advocacy is influencing Silicon Valley’s big tech corporations. Beginning in 2018, Apple, Google and Facebook had all added features designed to help users measure their time using those companies’ products and to manage their usage. Ultimately, however, it will be left to each user to be more aware of thier tech use time and to reduce it where possible.



Time Well Spent is a movement to align technology with our humanity.

Today apps and media compete in a race to grab our attention. Join a movement to:

- Live better with more empowering settings for our media and devices.
- Change incentives so media competes to improve our lives, not get eyeballs.
- Invent new interfaces that help us to make room for what matters.

Read more: https://humanetech.com/
https://www.wired.com/story/google-and-the-rise-of-digital-wellbeing/

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- If you are a user of a smartphone, tablet or laptop, do you know the way to track how much of screen time you spend on a daily or weekly basis (both Android and Apple phones now allow such tracking)?
- "Being mindful of how technology can distract and derail us helps us reap its benefits without letting the machines take over." Do you agree with this statement? Discuss.
- Have you checked your posture when seated and using a computer or laptop?
- Are you aware of the strain on your neck when looking down at a mobile phone screen for too long? Discuss what neck exercises and posture corrections are available.
- Visit Google's Digital Well-being website at https://wellbeing.google/ and find tools to help you understand and manage your tech use.

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- As technology becomes more and more integral to everything we do, it also impacts our bodies and minds, as well as our social life, in different ways. It is important to understand these impacts.
- Technology companies are recognising the impact of their tools and services, and devising ways for us to track - and control - how we use them
- We need not be enslaved by our digital tools. We can be smart about using digital technologies without them controlling our routine and social habits. One option is consciously self-regulating our digital habits.
- There are many simple actions we can take to reduce adverse impacts of prolonged use of mobile phones and computers.
- Most of us have not reached addiction levels in our use of digital tools, but many have a high dependency on them. Understanding the addictive nature of everyday digital technologies is the first step toward ensuring a reasonable balance between using technology without being addicted.

FURTHER READING

Digital responsibility website
http://www.digitalresponsibility.org/

Digital well-being website
https://digitalwellbeing.org/

Google Digital well-being website
https://wellbeing.google/

Office ergonomics: Preventing eye strain
https://healthengine.com.au/info/office-ergonomics-preventing-eye-strain

What is Digital Detox and how to start with it?
https://mrnoob.net/how-to-start-with-digital-detox/

MODULE 6

INCREASING DIGITAL LITERACY

INCREASING DIGITAL LITERACY

There are various definitions of digital literacy.

One simple definition is “the ability to find, evaluate, utilize, share, and create content using information technologies and the internet.”

Digital literacy covers a wide range of skills, all of which are necessary to succeed in an increasingly digital world.

Digital literacy builds on general literacy and reading skills. It provides people with an understanding of how digital technology functions, and how to use it effectively.

This includes critical thinking and assessment of information, familiarity with various digital devices, the ability to navigate the internet, and an understanding of issues associated with digital technology -- like data privacy and digital identity. These skills are now seen as essential.

Many who already use digital technologies -- such as tablets, smartphones or computers -- may already know how to browse the web, share images on social media, and do a basic search to find information. However, digital literacy today involves much more.

Digital literacy goes beyond technical knowledge and skills, and involves self-care, respectful behaviour and ethical conduct when using digital tools and going online. This is the vision for digital literacy that we need to promote in Sri Lanka.

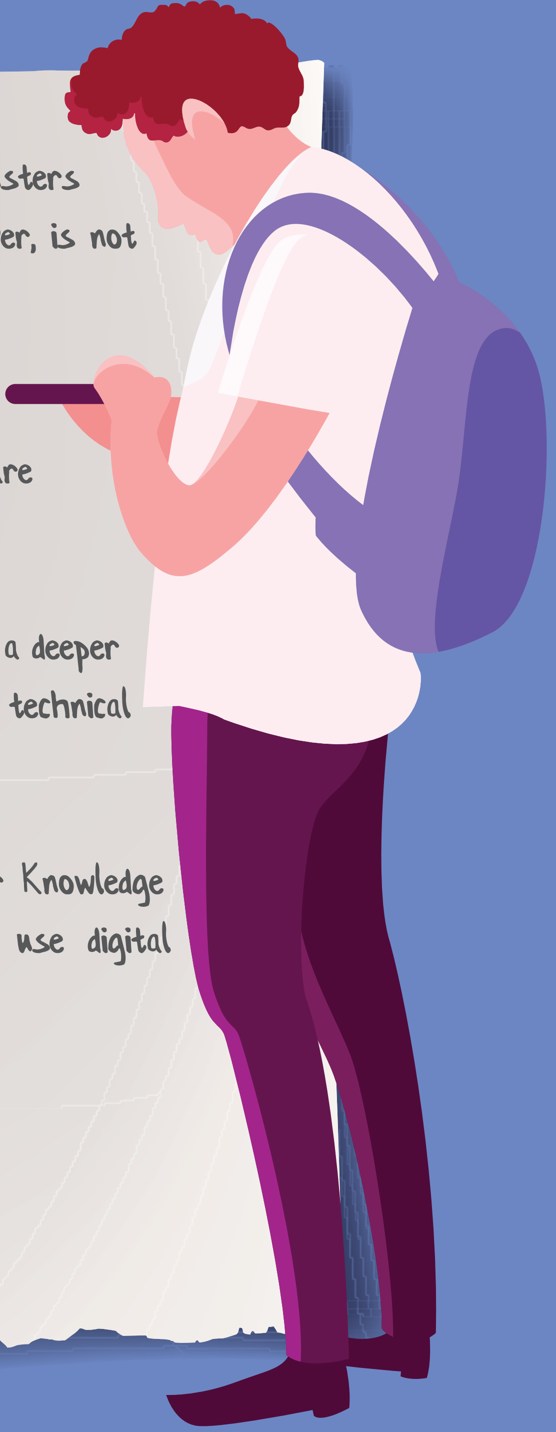
KEY TERMS

Digital literacy is an umbrella concept for important skill clusters whose names are often used as synonyms; their content, however, is not exactly the same.

ICT literacy refers to a set of user skills that enable active participation in a society where services and cultural offerings are computer-supported and distributed on the internet.

Technological literacy (previously called computer literacy) entails a deeper understanding of digital technology and comprises both user and technical computing skills.

Information literacy focuses on one of the key aspects of our Knowledge Society: the ability to locate, identify, retrieve, process and use digital information optimally.



Source: http://www.ictliteracy.info/

THREE FACETS OF DIGITAL LITERACY

Digital literacy skills have been categorized into three main areas: Finding and consuming digital content; creating new digital content; and communicating or sharing digital content.

Finding and consuming digital content: One of the most important components of digital literacy is the ability to not just find information, but also to evaluate that information. This means judging whether the information source is reliable and the information itself is trustworthy. The ability to weed out false information and find reliable content is an important survival skill today.

Creating new digital content: With so many free digital tools and services available online, we now have many different ways of creating new content that is interesting, visually rich, data driven and interactive. Acquiring these skills for content creation is a key part of digital literacy – it is useful for students, teachers, journalists and many other professionals who need to communicate information and ideas to various audiences.

Communicating or sharing digital content: Knowing how and when to share (or not to share) information we found online, and the content generated by ourselves, is also a valuable skill. Sharing has become easy with social media, but there are dangers of passing on wrong information (which becomes misinformation) or posting inappropriate comments or images online.

The ability to create and share content online is helpful in the networked society but learning how to do that while respecting other human beings, and adhering to copyrights and ethics is equally important.

DIGITAL LITERACY IN SRI LANKA

Digital literacy in Sri Lanka is still in its early stages. It is not to be confused with computer literacy because digital literacy involves a wider set of skills.

The Department of Census and Statistics (DCS) has been measuring computer literacy for more than a decade and has recently started measuring digital literacy as well. However, they use a narrow definition.

The Department defines computer literacy as the ability to operate a computer on one's own, irrespective of age. The computer literate population is expressed as a percentage of the total population aged 5 to 69 years.

The DCS definition of digital literacy is also basic one: a person (aged 5-69) is considered as a digital literate if he/she could operate computer, lap top, tablet or smartphone on his/her own. This definition does not look at any skills in using software or navigating the internet.

DCS conducts regular surveys to measure computer literacy and digital literacy. In 2018, DCS measured computer literacy rate in 28.3% (during the first six months). In comparison, the digital literacy rate for the whole population was 40.3% (males 44.5% and females 36.4%).

"Digital literacy is higher than computer literacy for all disaggregated levels, showing the drift from personal computer to smartphones/tablets," the DCS survey report noted.

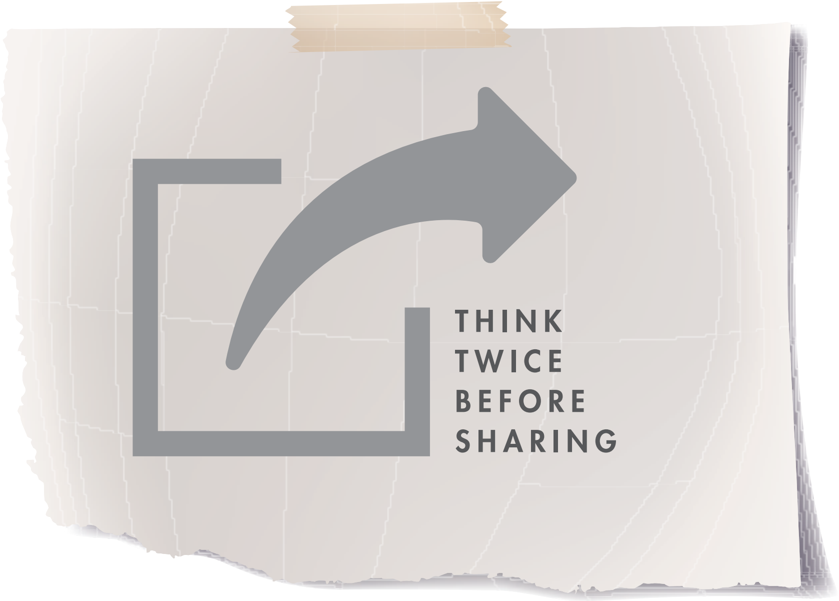
These surveys have found that the computer literacy and digital literacy skills are higher among those living in cities, and those younger in age. Digital literacy is not yet common among those over 50 years.

What DCS measures is a basic set of digital competencies, which are necessary ***but not sufficient*** for digital literacy.

For example, how many people who have access to the internet actually make use of the many online services available? And what is preventing them from making better use of these facilities?

A recent survey by the ICT thinktank LIRNEasia found that a majority of Lankan web users do not go beyond simple browsing to derive various economic and efficiency dividends the web provides. Only 40% of internet-users have done an interactive function such as a web search, posting or commenting on a website or social media, install an app, or create a log-in for using a particular web service.

The main reason, this survey found, was that many users did not have the necessary knowledge and skills – or were afraid of venturing beyond a few familiar websites like Facebook. This highlights major gaps even among those who can operate digital devices and access the internet.



[1] http://www.statistics.gov.lk/education/ComputerLiteracy/ComputerLiteracy-^{2018}Q^{1}-Q^{2}-final.pdf
[2] https://lirneasia.net/after-access

DIGITAL COMPETENCIES

Internationally, discussions have been taking place about what digital skills should be promoted through schools, universities and other means.

The European Digital Competence Framework for Citizens, known as DigComp, offers a tool to improve citizens' digital competence. DigComp was first published in 2013 and has become a reference for many digital competence initiatives. It was revised in 2016 as DigiComp 2.0, which has since been adopted by UNESCO as a global framework.
The competencies listed under DigiComp 2.0 are the following:

COMPETENCE AREA	COMPETENCE
1. Information and data literacy	1.1 Browsing, searching and filtering data, information and digital content 1.2 Evaluating data, information and digital content 1.3 Managing data, information and digital content
2. Communication and collaboration	2.1 Interacting through digital technologies 2.2 Sharing through digital technologies 2.3 Engaging in citizenship through digital technologies 2.4 Collaborating through digital technologies 2.5 Netiquette 2.6 Managing digital identity
3. Digital content creation	3.1 Developing digital content 3.2 Integrating and re-elaborating digital content 3.3 Copyright and licences 3.4 Programming
4. Safety	4.1 Protecting devices 4.2 Protecting personal data and privacy 4.3 Protecting health and well-being 4.4 Protecting the environment
5. Problem solving	5.1 Solving technical problems 5.2 Identifying needs and technological responses 5.3 Creatively using digital technologies 5.4 Identifying digital competence gaps

Not everyone needs to acquire all the competencies, of course. But as education, business, governance and other aspects of life become digitally transformed, more and more of these competencies would be needed.

Digital literacy does not mean everyone has to become a technical person in information technologies. Consider this simple analogy. People who own a personal vehicle – whether it is motorcycle, three wheeler, motor car or another type – are expected to know basic care for their vehicle and also how to drive it while respecting road rules and rights of other road users. Vehicle owners are also expected to attend to basic maintenance needs (such as changing a wheel), but not any major repairs. For anything advanced, a motor mechanic's services would be required.

Similarly, users of digital tools and services need to have the knowledge and skills for safe and productive use, respect for other users and knowing when and where to seek help. If there are any hardware or software problems, they can seek help from technical experts.

[1] Details at: https://web.eecs.umich.edu/~cscott/rsi.html

RESPONSIBLE ROAD USE AND DIGITAL USE: A COMPARISON

Roads connect people across physical spaces, just like the web helps connect its users across cyberspace. Everyday millions of people use roads – as pedestrians, passengers in public transport, or as drivers controlling their own vehicles. Most of them complete their journeys without any incident, yet road traffic accidents have been increasing in Sri Lanka (in 2018, a total of 3,164 were killed in such accidents, and thousands more were injured, some of them disabled for life.)

Road accidents happen due to the carelessness of drivers and pedestrians, and also due to poor road conditions and bad weather. Road rules and their strict enforcement can reduce (but not totally eliminate) these accidents. Road safety is not just a matter of laws and penalties: it also requires better designed roads, greater public awareness and individual responsibility by all road users.

Now imagine a situation where we avoid stepping on to the roads because there is a chance of being involved in an accident? Instead, we take precautions and some risks too: the benefits of road use are much greater than non-use.

Imagine, also, a situation where the government shuts down all roads because road accidents are increasing. That is not a viable situation, even for a few hours: the authorities have to find other ways to manage the problem.

It is the same with the web and digital tools. There are some risks involved, but users can minimize them by being better aware, and by taking certain precautions (like strong passwords and two-step authentication for their digital accounts – as explained elsewhere in this toolkit).

And yes, just as roads are sometimes used by criminals and perverts, the web can also be used by persons trying to use it for anti-social or criminal purposes. The right response is not to avoid using the web and all its services, but to know how to be safe and where to report and seek help if you experience these.

HOW TO IDENTIFY FALSEHOODS

‘Fake News’ is a popular phrase, but not a very helpful one to understand the complexity involved, because falsehoods come in different shapes and forms:

- disinformation (deliberately spreading falsehoods);
- misinformation (unknowingly spreading falsehoods); and
- mal-information (falsehoods spread with intent of causing societal harm)

False information and manipulated images have been around for centuries. In the 21st century, however, the spread of web and social media use has made it much easier to originate and/or share falsehoods. Some of these can cause real harm: they can undermine public health, aggravate racial or religious tensions, confuse voters at elections, and even threaten social harmony by triggering violence.

It is important to remember that falsehoods are originated and spread by mainstream media too. Sri Lanka’s newspapers, radio and television have a long history of spreading disinformation for political, ideological or other reasons.

The challenge is to help citizens spot dis/mis/mal information in both mainstream and social media (and also when it spreads through rumours).

[2] https://www.pewinternet.org/2012/02/29/millennials-will-benefit-and-suffer-due-to-their-hyperconnected-lives/

Here are 10 tips on how to spot fake news, compiled by the UK newspaper ***The Telegraph.***

- **Beware of stories that don’t make sense:** One of the key signs of fake news is that the stories are highly improbable.

- **Check the name of the news site that published it:** The names of sites publishing news stories are often a hint that stories may be fake. Be a little more careful of websites that you haven't heard of before. Unfamiliar sites built to sound like news organisations are behind many fake news stories.

- **Beware of fake website addresses:** Some sites may try to impersonate real news outlets with domain names which seem similar but have slight differences.

- **Look out for headlines which don’t match the story:** Make sure the headline and the story match up. False news sites often have headlines in all-capitals that capture the attention with emotional claims – which don’t match the copy that follows if you actually click to the news site.

- **Check the date:** Look out for suspicious dates. False news stories often include timelines which make no sense or contain the wrong dates for established events. For instance, images purporting to be of a 2016 terror attack in Brussels were actually from a 2011 attack on Moscow’s Domodedovo Airport.

- **Look for unusual spellings and mistakes:** Often, the sign that news is fake is that it is of low quality, with spelling errors and an over-use of capitals. Real news sources will employ editors to remove these errors and ensure accuracy.

- **Be wary of headlines which are trying to provoke anger:** Headlines that seek to provoke anger are a sign of fake news. It does not matter what side you are on, the purpose of fake news is often to drive two groups apart and fuel prejudice and intergroup conflict.

- **Look out for hoaxes spread by fake celebrity accounts:** Sometimes stories can spread online after being shared by a fake celebrity, a social media account designed to impersonate a real person.

- **Google-search the images:** Fake news sites will often use criminal mugshots from unrelated stories or doctored images. Google-search the images to check for their veracity against other legitimate news sites and to see where they came from.

- **If you are unsure, double check with a source you trust:** Fake news stories will often appear on just one site, so if you're unsure, double check via a news source you know and trust, says Moy of Full Fact. "When it matters, double check. Particularly when it comes to health or other life decisions, always use a trusted source."

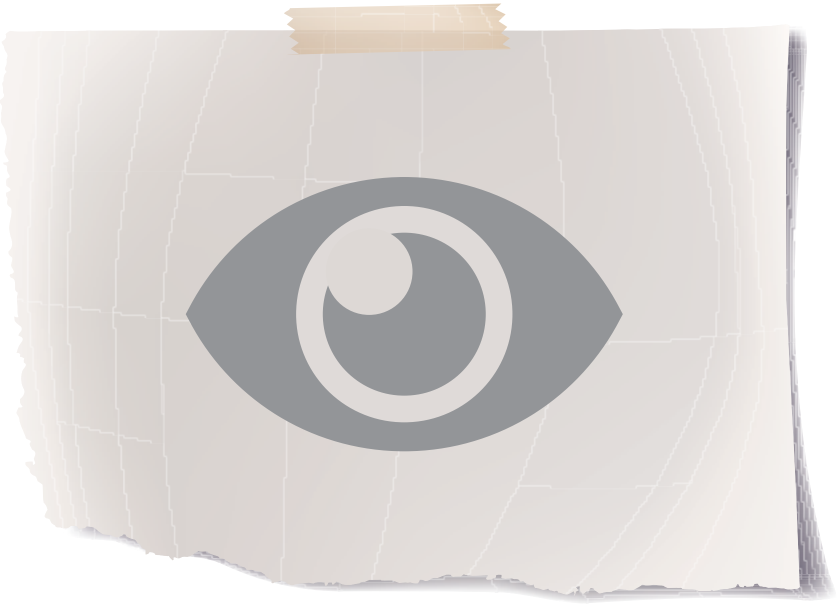
[3] https://www.telegraph.co.uk/technology/information-age/how-to-spot-fake-news/

A VISION FOR DIGITAL LITERACY

As we said earlier, just having the skills to operate digital tools is not enough. To make the best use of digital technologies and the web, users need to have the right attitudes and a clear sense of purpose too. They need to take care of themselves and respect others when using digital technologies.

In Sri Lanka, some people have various misconceptions about the internet – for example, viewing it as an inherently unsafe space, and considering social media as particularly dangerous and exploitative.

Any technology can be used well for the benefit of individuals and society as a whole. The same technology can also be misused by some for exploiting or harassing others, thus creating problems. We don't need to stop using any technology simply because some are misusing it. Instead, we as a society need to introduce adequate safeguards, increase user awareness and have regulatory systems to deal with those who misbehave or misuse it.



CASE STUDIES

CASE STUDY 1: PROMOTING DIGITAL LITERACY AMONG YOUTH

Sarvodaya-Fusion is a social enterprise focused on ICT for development with the mission "e-empowerment of rural communities". It is a subsidiary of the Sarvodaya movement, the largest charity non-profit organization in Sri Lanka, founded in 1958.

For the past several years, Fusion has successfully designed and delivered programmes providing digital literacy, digital access and digital benefits.

One of Fusion's key programmes is called 'IT Yahamaga' (or Right Use of IT), an
initiative that takes digital literacy to school children in Sinhala and Tamil languages. It is designed to create awareness among school children, teachers and parents on latest ICT technologies and tools, their positive usage, the security and control aspect to be safe in a digital world and the responsible handling of such ICT tools.

IT Yahamaga's interactive training sessions include training on the safe and responsible use of the internet and contains topics that teach online users how to think critically online and effectively differentiate credible information from suspicious ones. It also includes empathy as a key value to express online with the aim of not just creating a safer and informed community but one which embraces multiple perspectives and respects differences of opinion.

In recent months, Fusion has also launched a social media campaign countering hate speech and misinformation on social media. Their core message is: Think before you share!

Read more: https://fusion.lk/
https://www.facebook.com/sarvodaya.fusion/

DO NOT
EXCHANGE
YOUR PERSONAL
INFORMATION
WITH STRANGERS
ON SOCIAL MEDIA
fusion
Sarvodaya CT4D Movement
PAY ATTENTION & CAREFULLY
SELECT YOUR FRIENDS
ON SOCIAL MEDIA
fusion
Sarvodaya CT4D Movement

CASE STUDY 2: BUILDING DIGITAL LITERACY AT THE GRASSROOTS

Mahawilachchiya is a remote and rural area in Anuradhapura district, located close to the Wilpattu National Park. Yet the children of this village were connected to the internet and creating their own digital content from the early 2000s -- well before many city schools had internet facilities.

This was due to the efforts of Horizon Lanka Foundation, a pioneer in taking information and communication technology (ICTs) to the grassroots. Founded in 1998, it has been instrumental in teaching English and ICT to thousands of youth in rural Sri Lanka using innovative methods.

Horizon began as an after-school voluntary activity providing rural school children with further education in English and ICT. Its founder Nanda Wanninayaka was a teacher of English in government schools who soon left his job to devote all his time and energy to Horizon. He raised donations from local and foreign well-wishers for the non-profit organization which has pioneered new ways of raising digital literacy at the grassroots.

“I find that many parents and teachers in Sri Lanka are scared of the internet and smartphones due to media reports of various misuses. Some families prevent children from using any digital tools. This deprives such kids the opportunity to learn how to survive in tomorrow’s information-driven society,” says Horizon founder Wanninayaka.

He advocates the safe use of digital tools and the internet, instead of their non-use.

Many of Horizon's former students have gone on to graduate from universities and secured jobs in the IT industry. Some have even started their own business process outsourcing (BPO) – taking outsourced data processing work from companies in Colombo and overseas.

Horizon website says its commitment is "to make rural Sri Lanka as technologically evolved as any metropolis whilst retaining its culture and sense of community. With ICT and English education at the core of our activities, we strive to bridge the opportunity gap in Sri Lanka."
Horizon has recently started setting up franchised schools in other areas of Sri Lanka.

Read more: http://www.horizonlanka.org/en/about-us/our-story/
https://www.facebook.com/horizonlankafoundation/

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- Can you self-assess which digital competencies you already have, according to DigiComp 2.0 list?

- What does digital identity mean to you? How do you manage or safeguard your digital identity? Have you ever had a situation where somebody else tried to pose as you in social media or elsewhere online – and if so, what action did you take?

- What information sources do you trust, and why? When you come across something suspicious (or too good to be true), what steps do you take? How do you verify information? Discuss.

- When you create digital content, how do you find images? Do you just take any image from the web, or do you consider copyright (also known as intellectual property)? In which ways can you respect intellectual property of content you find online?

- All government schools have banned students from brining mobile phones to the classroom. Do you agree with this restriction? Discuss the pros and cons of allowing minors (i.e. all those below 18 years) to use smartphones with web browsing capability.

- The government has decided to provide all Advanced Level students and their teachers with tablets. Some welcome this decision while others are not so sure. Discuss the benefits of students having their own tablets for classroom work, and how to manage potential risks and hazards.

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- Computer literacy and digital literacy are related but they are not the same thing.
- Digital literacy involves mastering the skills to use digital tools and the web effectively, but it is also much more: it calls for knowing how to use these services in a safe, respectful and ethical manner.
- Sri Lanka's digital literacy levels are still low, and most of those who have these skills are in the younger age groups.
- Digital literacy is going to be a survival skill in the 21st century as we are exposed to more information, digital services as well as digital risks and opportunities.
- Digital literacy is not something limited to schools or universities. Anyone can learn or enhance these competencies at any stage in life. Indeed, as technology keeps evolving all the time, everyone needs to be updating or refreshing their digital literacy.

FURTHER READING

DigComp 2.0: The Digital Competence Framework for Citizens (European Union, 2016).
https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model

A Global Reference Framework on Digital Literacy Skills for Indicator 4.4.2 (UNESCO, 2018)
http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf

Digital Literacy Fundamentals (Canada's Centre for Digital and Media Literacy)
http://mediasmarts.ca/digital-media-literacy/general-information/digital-media-literacy-fundamentals/digital-literacy-fundamentals

How to spot fake news, a guide by the British Council
https://learnenglish.britishcouncil.org/intermediate-b1-reading/how-to-spot-fake-news

What is fake news and how can you identify it? A guide by the BBC
https://www.bbc.com/news/av/technology-46149888/what-is-fake-news-and-how-can-you-identify-it

MODULE 7

ADVANCING DIGITAL ACTIVISM

MODULE 7

ADVANCING DIGITAL ACTIVISM

Activism! It means a person or group acting publicly and peacefully on an issue of shared concern.

The issue may be social, political, environmental or one related to public health and safety. Activists want a change in the current situation which they are not happy about. Activists may advocate change at community level, with local government, national government or sometimes internationally.

Digital activism, also known as cyber activism, is a form of activism that uses the internet and digital technologies as key tools for awareness raising, mobilization and action. As with all other kinds of activism, it needs to be pursued peacefully and ethically.

In this chapter, we briefly explore the various kinds of digital activism being pursued in Sri Lanka and elsewhere. Our aim is to identify some common strategies used by individual activists, as well as by civil society groups including youth organizations.

We will also see how the internet enables new kinds of activism by enabling the spontaneous forming of groups of persons who share the same concern.

We also emphasize that successful activism cannot happen entirely online. It requires a healthy mix of online and offline approaches.

KEY TERMS

Advocacy: An activity by an individual or group that aims to influence decisions within political, economic or social systems. Advocacy includes activities to influence public policy, laws, regulations or budgets by using facts, arguments, media use, and other kinds of messaging to government officials and/or the public.

Activism: The policy or action of using vigorous campaigning to bring about social or political change.

Clicktivism: The practice of supporting a political or social cause via the internet by means such as social media or online petitions, typically characterized as involving little effort or commitment.

Slacktivism combines the words "slacker" and "activism" to refer to simple measures used to support an issue or social cause involving virtually no effort on the part of participants. Slacktivism critics argue that these actions lack genuine commitment and fail to produce any tangible effect.

Source: http://www.ictliteracy.info/

ACTIVISM: STORY SO FAR

Activism is nearly as old as civilization itself. The urge for change – and the need to collectively organize and advocate it – has driven women and men to activism for centuries.

Activism is much more than agitation. Indeed, the history of activism around the world shows that the most effective activists are those who analyzed problems, listened widely and identified solutions that they then advocated through different methods – including public communication, peaceful demonstrations, marching, picketing and boycotting of certain products. Often, activists collaborate with other like-minded groups and, where necessary, engage in (ideally, transparent) negotiations with governments or corporations whose change was being demanded.

An outstanding historical example of effective activism is the life of Mahatma Gandhi (1869 – 1948). Trained as a lawyer in England, he spent over two decades practising law in South Africa where he was closely associated with struggles for social justice against racial and economic injustices. A transformed Gandhi returned to India in 1914, and soon became a leader of the movement against the British rule of India.

The foundation of Gandhi's activism was nonviolent protest (satyagraha) and civil disobedience to achieve political and social progress. For him, nonviolence was not simply the absence of physical violence. Self-rule and radical democracy -- in which everyone participates in the governance process -- were also important parts of it. In pursuit of his goals, Gandhi was an orator, writer, journalist and peaceful demonstrator. He communicated with the British rulers without compromising his ideals.

Years later, Martin Luther King Jr. (1929 – 1968), who had met with Gandhi, would employ similar ways of nonviolent resistance during the civil rights movement with the goal of enforcing constitutional and legal rights for African Americans that white Americans already enjoyed.

For today's activists and protesters, Gandhi and King's political strategies could provide some valuable lessons. The peaceful resistance that the two pursued was more effective in exposing hard truths about injustices.

LESSONS FROM MAHATMA GANDHI

Mahatma Gandhi lived by five pillars of non-violence: respect, understanding, acceptance, appreciation and compassion. "Although Gandhi was as flawed a human as any of us, he did his best to live by those pillars," writes Arun Gandhi, a grandson, in his 2015 book titled 'The Gift of Anger and Other Lessons from My Grandfather Mahatma Gandhi'.

Read more at: https://www.beliefnet.com/inspiration/the-lessons-of-mahatma-gandhi.aspx

ACTIVISM AND COMMUNICATION

Making good use of communications tools has always been a key part of activism. As technology advanced, more tools became available for activism.

Activism started through oratory means, with public speeches calling changes or social reforms. After the printing press was invented, that enhanced the reach for activists who started using handbills, leaflets and pamphlets summarizing their positions and calls to action.

As different type of mass media emerged – starting with newspapers and magazines, and then radio and television – activists found ways of using these media to amplify their messages. However, accessing the mass media has often been a challenge for activists as media companies are controlled by the state or corporate owners (and editors) who decide which messages are allowed, and how.

Digital and web tools are the latest additions to the activist toolkit. These enable any individual with internet access to self-publish bypassing the 'gatekeepers' of owners and editors. Activists and reformers were quick to realize and seize this potential.

The web is an inherently interactive environment, and all activists need to recognize this. It means engaging in two-way communications, driven by public debate and regular engagement with virtual communities – including detractors and critics, if any.

[1] What Gandhi can teach today's protesters. The Conversation, [2] October ^{2017}. http://theconversation.com/what-gandhi-can-teach-todays-protesters-^{83404}

ACTIVISM ONLINE

Digital and online activism involves a blending of campaigning, marketing and community building using various web platforms. Sometimes it extends to raising public donations for a specific cause (such as disaster relief).

In the early days of the web during the 1990s, activists used the new medium mostly for disseminating information and advocacy positions: websites (and later, blogs) gave them a potentially global reach at a low cost.

After social media emerged in the 2000s, digital activism evolved to become more interactive and complex. Different ways of mobilizing people became possible -- through campaigns, online petitions, virtual meetings, and virtual sit-ins, etc.

While the mainstream media is still an important outlet reaching out to some sections of society, more and more activism is happening online today.

Beyond outreach and mobilization, digital tools and web platforms also allow activists spread across space and time to plan and organize around shared goals and issues.

Globally, campaigns like #BlackLivesMatter, #MeToo and #ClimateStrike have been largely driven on social media. Yet significant actions are also being taken through physical activities like street marches and public gatherings.

A key learning from dozens of social and political activism efforts in recent years is that success depends on a healthy mix of online and offline action. Peaceful street demonstrations, marches and sit-ins at public spaces still matter, and they generate lots of photo opportunities for both social media and mainstream media.

A key challenge for activists using social media is how to sustain public interest over time. Online interest can build up fast, but it can also dissipate fast. Staying on with a single issue or cause is hard when news breaks round the clock and so many topics distract people.

Finally, it is important to remember that digital activism is much more than the use of technology. The context of digital activism refers both to the digital technologies used in a given campaign and to the economic, social and political context in which such technology use occurs.

Digital technological infrastructure -- the combination of networks, code, applications and devices -- is only the starting point. It is the differences in economic, social, and political factors in each situation or country that ultimately determine how much activists can succeed in using digital tools for public causes. Therefore, understanding your social and political realities is an important first step.

ACTIVISM ONLINE: RECENT EXAMPLES

#BlackLivesMatter is an international activist movement, originating in the African-American community, that campaigns against violence and systemic racism towards black people especially in the United States. It started in 2013 after many instances of police brutality and discrimination.

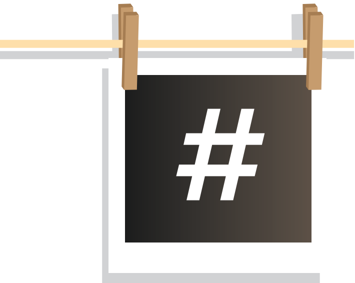
#ClimateStrike is an international movement of school children who take time off from classes to take part in demonstrations demanding action to prevent further global warming and climate change. It began when Swedish schoolgirl Greta Thunberg staged a protest outside the Swedish parliament in August 2018. It has since spread worldwide involving youth and many others from all walks of life.

#MeToo is a worldwide movement against sexual harassment and sexual assault. The movement began to spread virally in October 2017 as a hashtag on social media. (Details in Case Study 5 below.)

ONLINE ACTIVISM STRATEGIES

Successful online campaigners have found various creative strategies to sustain their advocacy and activism. Here are three examples.

HASHTAGS



A hashtag is a common sorting device that makes it possible for others to easily find messages with a specific theme or content on many social media platforms such as Twitter, Instagram, Facebook, Reddit and YouTube.

A good hashtag needs to be short, punchy, memorable and distinctive (it is always good to search and see if your proposed hashtag is already being used by any other group elsewhere).

There are common hashtags widely used to denote Sri Lanka: #lk, #lka, #sl and #SriLanka.
In recent years, using common hashtags like #FloodSL, #FloodLK and #SLFloods, citizens mobilized voluntary efforts for rescue and relief after major flooding incidents. #PresPollSL was widely used in connection with the presidential election of January 2015 and is being revived in time for the next presidential election in late 2019. During the 51-day political crisis from 26 October to 16 December 2018, one of the most widely used hashtags was #CoupLK (suggesting the transfer of power was illegal), while other hashtags like #ConstitutionalCrisisLK and #PoliticalCrisisLK were also used.

Anyone may coin a new hashtag, but only some hashtags become popular or 'go viral' by many users adopting it. Hashtags emerge from among social media users themselves, and digital activists are learning how to use this simple device to connect their various posts and messages.

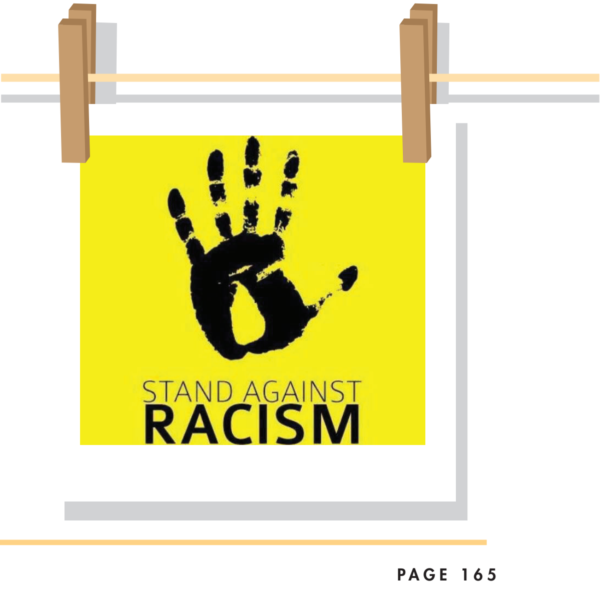
MEMES

A web meme usually takes the form of a static image, animated (GIF) image or video, and is meant to convey an idea quickly through mimicry, humour or satire. The creators of web memes mostly remain anonymous, and only some memes spread rapidly through multiple sharing on social media.

Memes can be rough and dirty, or they can be works of art with sophisticated graphics. It is the idea and its clever expression that matters more than presentation.

Memes originated in popular culture, but social and political activists quickly seized its potential for public interest communications. From gender empowerment and anti-corruption action to clean elections and climate activism, memes have become an integral part of digital activism today. As with hashtags, success of a given meme depends on creativity and timeliness.

A good example of a meme is the palm sign with 'Stand Against Racism' which first emerged after anti-Muslim violence in Aluthgama in June 2014. While its creator remained unknown, this aptly captured the sentiment of peace-loving majority of Lankans who shared it widely with calls for racial harmony, compassion for the affected and restraint by everyone.



ONLINE PETITIONS

Online petitions are another tool available to activists if they live in a society where public opinion is valued and respected by government officials and corporate entities.

Visitors to an online petition can sign the petition by adding their details such as name and email address. Typically, after a petition gathers a sufficiently large number of signatories, it may be delivered to the subject of the petition which can be a political leader, government official, or a corporation.

Most petition websites also allow people to sign up and initiate new petitions. There are several major web initiatives featuring online petitions, such as Change.org, Avaaz.org and iPetitions.com. Avaaz is a US based nonprofit organization launched in 2007 that promotes global activism on issues such as climate change, human rights, animal rights, corruption, poverty and conflict.

DATA VISUALIZATION

Activism can become more effective with the sound analysis of data related to the issue or cause being advocated. However, most people can’t relate to numbers that need to be presented in ways easy to understand.

Data visualization is the graphical representation of information and data. By using visual elements like charts, graphs and maps, data visualization tools provide an accessible way to see and understand trends, outliers, and patterns in data. Powerful infographics can make campaigns come to life for the broadest possible audience.

Translating dry reports and databases into a format that resonates with human beings is one of the main purposes of data visualization. When done well, it can not only bring out the insights found in the data, but also humanize the issue in question.

"WHETHER WE'RE SWAMPED BY IT OR STARVED OF IT, THE VALUE OF INFORMATION DEPENDS ON ITS QUALITY, AND ITS USEFULNESS DEPENDS ON OUR ABILITY TO COMMUNICATE IT SUCCESSFULLY. AS ACTIVISTS, WE CAN'T SIT AND WAIT FOR PEOPLE TO WADE THROUGH SIXTY-PAGE REPORTS. TO INFLUENCE PEOPLE WE MUST MAKE STRONG ARGUMENTS AND COMMUNICATE THEM USING STRONG EVIDENCE. WELL TIMED, RIGOROUS AND WELL PRESENTED INFORMATION IS THE GREATEST ASSET ACTIVISTS POSSESS." -

VISUALISING INFORMATION FOR ADVOCACY, 2013
BOOK BY TACTICAL TECHNOLOGY COLLECTIVE

DIGITAL ACTIVISM IN SRI LANKA

Sri Lanka has a long history of social, political and environmental activism going back to several decades. In recent years, individuals and groups concerned with various issues – from political reforms and social justice to animal welfare and public health – have started using websites, blogs, online petitions, social media and other digital tools.

As Freedom on the Net 2018 report on Sri Lanka, compiled by the US-based research and advocacy group called Freedom House, noted: "The web has provided an avenue for robust digital activism and engagement on political issues in Sri Lanka, although most campaigns progress in fits and starts. Many are hitched to specific short-lived events, crises, or stalled political processes, and campaigners are generally unable to gather the momentum needed to drive meaningful change and long-term participation. However, a number of social media campaigns occurred during the reporting period (2017-18)."

Digital activism in Sri Lanka has been organized around shared hashtags as well as popular slogans. Here are a few among many examples:

- #IVotedSL online campaign was started to encourage citizens to participate in two key elections, i.e. the presidential election of January 2015 and Parliamentary election of August 2015. It was revived during the local government elections in February 2018, together with #LGPollSL, with many first-time voters sharing photos of themselves (inked finger indicating having cast their vote).

- When the Right to Information (RTI) law was unanimously passed by Parliament in June 2016, it marked the culmination of an advocacy campaign that started in 1994. Most of that advocacy was done offline, but since the law became a reality, activists have been using mainstream and social media to raise awareness about the new right and to encourage more citizens to exercise it. The common hashtag #RTIsl is being used.

- Human rights activists and civil society groups have been using #DisappearedSL to track and support the protests by families of the disappeared across the north and east, and to demand justice. Amnesty International also uses the hashtag #StillNoAnswers.

- Promoting ethnic and communal harmony has been the basis of activism both online and offline that brought together many individuals and groups to renounce racism and discrimination based on race or religion.

- Preventing sexual harassment in public transport and at work places has become a priority as data has revealed high levels of these practices. In response, awareness and advocacy campaigns have been launched both online and offline. The UN Population Fund (UNFPA) collaborated with local partners on the #DoesSheTravelSafe campaign in 2018, while in early 2019 Oxfam Sri Lanka and partners launched #NotOnMyBus and #CreateAScene social media campaign calling for bystander intervention as a solution against sexual harassment of women and girls.

Not every attempt at digital activism succeeds. For example, a social media campaign organized around #NewConstSL was intended to drive conversations around constitutional reforms, but it has failed to gain much interest as the reform process itself stalled.

Sometimes activists can digitally ‘crash somebody else’s party’ to raise a neglected concern. An example is how, in 2017-18, the citizen journalism platforms Groundviews, Vikalpa and Maatram used the #Celebrate150years hashtag marking 150 years of Ceylon Tea to highlight the plight of the Up-Country Tamil community – who remain the most deprived segment of the population. (Note, however, that it can work both ways: activist-originated hashtags can sometimes be hijacked by those opposing their advocacy positions.)

More Lankan examples can be found among the case studies below.

CRITICISM OF DIGITAL ACTIVISM

There is some criticism of digital activism, and their arguments are worth noting.

Social media ‘clicktivism’ creates more apathy than empathy, they say, pointing out that true social change requires more than merely liking or sharing a social media post for a worthy cause. One critic says this leads to a form of “one-click rent-a-mob” – enabling ill-informed and disconnected instant electronic communication instead of genuine political discussion and interaction. Another critic says while it is easy to ‘click’ about issues on social media, it is just as easy to disengage online. There is also criticism that online petitions can over-simplify complex ethical questions.

In their defence, digital activists say the web and social media are additional tools to be used by activists and are not ends in themselves. Yes, they are the imperfect tools and the best results are achieved when they are used appropriately and thoughtfully.

Some data analysis done in the US shows ‘Clicktivists’ are twice as likely to volunteer, twice as likely to ask for donations, two times more likely to take part in an event and four times more likely to encourage others to engage.

For us in Sri Lanka, where only a third of society is using the internet, activism should always combine the offline with online.

ETHICS OF DIGITAL ACTIVISM

Activism – online and offline -- needs to be conducted within an accountable, transparent and ethical framework. Having good intentions does not justify resorting to dubious or self-serving practices.

For example, some online petitions have been exposed as a way of acquiring people's email addresses to later sell them for a profit to digital marketing companies. And certain fund-raising campaigns online have later diverted most of what they collected to cover running costs of charities.

Social activists are entitled to their own political views and political party loyalties. However,
in public interest advocacy and activism, it is best to rise above political divides. It would be unethical for political parties to influence or coerce a social activism campaign for political gains. Similarly, advocating a public cause does not justify any activist using threatening or hateful language on social media.

> "ONLINE ACTIVISTS NEED TO WORK ON A WAY TO IMPROVE THE QUALITY OF THE DISCOURSE BY DEVELOPING HABITS AND OPERATING UNDER STANDARDS TO MAKE THEM MORE ETHICAL. LOSING SIGHT OF THE GOAL TO DO GOOD BY CALLING FOR VIOLENCE OR ENGAGING IN 'SOCIAL MEDIA WARS' CAN BE VERY PROBLEMATIC FOR THE ISSUE OR CAUSE BEING ADVOCATED FOR."-
>
> ETHICS AND SOCIETY BLOG BY FORDHAM UNIVERSITY

ACTIVISM AS A CONTINUUM

Finally, we need to remember that an activist's task is never finished: there is always more to be done. Activism needs persistence, tenacity and ability to take the long-term view.

As life-long activists for human rights, social justice or environmental conservation know well, some campaigns are more successful than others in changing a specific policy, law or action. Narrowly defined activist demands – such as suspending a contentious law or withdrawal of a controversial product – are more likely to succeed than calls for difficult reforms such as phasing out dependence on petroleum and coal to contain global warming.

This reality is true for digital activism as well. While specific successes are to be celebrated, activists need to stay engaged for social, political and other reforms that take time, effort and dialogue. Some reforms take generations to be completed, and activist vigilance is needed to guard against societies or political systems from backsliding.

As US writer Malcolm Gladwell says, "activism that challenges the status quo – that attacks deeply rooted problems – is not for the faint of heart."

CASE STUDIES

CASE STUDY 1: ABOLISHING SLAVE TRADE IN BRITISH EMPIRE

One of history's most persistent social activists was William Wilberforce (1759 – 1833), a British politician, philanthropist and leader of the social movement to abolish the slave trade in which British-owned ships were carrying black slaves from Africa, in appalling conditions, to the West Indies to be bought and sold.

As a campaigner, he first found out what was happening. He also amassed incriminating evidence – including eye witness testimonials -- about the mass-scale abuse of human rights taking place in both Africa and on the high seas transporting captured African slaves. He then wrote and spoke across Britain using facts and figures, as well as appeals to human emotions. He managed to collect over 300,000 signatures in a petition from ordinary people calling for abolition of slavery — which countered the political argument that the ordinary people didn't care about far away abuses.

He worked with progressive Christian leaders and used churches to spread his message. He entered Parliament to advocate on this single issue. He organized consumer boycotts of sugar produced in plantations that used slave labour.

It was not until 1807 — full 20 years after Wilberforce started his campaign — that the British Parliament passed Abolition Bill and banned the slave trade. He then worked to ensure these laws were properly enforced and that slavery was abolished everywhere in the British Empire.

'Amazing Grace', a 2006 British-American biographical film directed by Michael Apted, is based on the life and work of William Wilberforce.

The strategies that Wilberforce used over 200 years ago are still valid in the digital age.

Read more: https://www.christianitytoday.com/history/people/activists/william-wilberforce.html

CASE STUDY 2: DARK IS BEAUTIFUL

In many parts of South Asia -- including Sri Lanka – there is a social belief that the value and beauty of people is enhanced by the fairness of their skin. Darker skinned individuals were socially and economically disadvantaged during British rule in India, and the colonial attitude of 'colourism' has continued decades after the British left.

Women and girls are the most affected by society's bias towards fairer skin. It has given rise to a multibillion dollar industry encompassing not only 'whitening' cosmetic creams but procedures such as skin bleaching, chemical peels, laser treatments, steroid cocktails and intravenous injections – all posing varying levels of health risks.

The 'Dark Is Beautiful' campaign was launched in 2009 as an awareness and advocacy campaign to fight this colourism. It seeks to draw attention to the unjust effects of skin colour bias, shaped by societal attitudes and reinforced by media messages that are undermining the self-worth of millions of people from all walks of life.

The campaign was started by Kavitha Emmanuel through a non-profit organization called
Women of Worth (WOW). It has received celebrity endorsement, most notably by the Bollywood actor Nandita Das. The campaign runs media literacy workshops and advocacy programmes in schools to convey messages of self-esteem and self-worth to young children.

A blog provides a forum for people to share their personal stories of skin colour bias. Social media is being used to raise general awareness and stimulate discussions.

During the decade since it started, the Dark Is Beautiful campaign has gained international recognition and been emulated in several countries that have a fair skin bias. The Advertising Standards Council of India tackled skin-based discrimination in 2014 by banning advertisements depicting people with darker skin as inferior. But some such products are still marketed.

Kavitha Emmanuel believes that people are more aware of the issue and hopes that the next generation will see things differently – not just in India but across the world.

Read more: http://www.darkisbeautiful.in/
https://thewire.in/business/skin-lightening-industry

CASE STUDY 3: HASHTAG GENERATION

Hashtag Generation is a youth-based and youth-led advocacy group in Sri Lanka. It was founded in June 2015 “to fill the vacuum that exists in meaningful youth civic and political participation in Sri Lanka”.

They identified social media as an efficient platform to raise awareness and catalyze dialogue on important issues through creative, easy-to-understand and youth-friendly digital illustrations and advocacy campaigns. However, as the team expanded, Hashtag Generation also undertook several offline campaigns and projects.

Hashtag Generation has distinguished itself by always working in Sinhala, Tamil and English, and by having an imaginative, graphics driven approach to all their public communication. They have been active on several fronts, always bringing youth perspectives into key national debates and processes. These include promoting ethnic harmony and transitional justice, addressing violence against women and girls (#HerSafeSpace), advocating equality for sexual minorities, and supporting women’s political participation, especially after a law revision required 25% of candidates nominated by political parties to be women.

Read more: https://www.facebook.com/hashtaggenerationsl/

CASE STUDY 4: BAKAMOONO.LK

Bakamoono.lk is a website and social media brand that promotes respect for self, respect for the other, and respect for difference. As they describe themselves, “Bakamoono.lk is about being sensible, even wise, in our dealing with issues around relationships, sexual and reproductive health, HIV, gender, and our right to be who we are.”

The team that runs bakamoono.lk is led by The Grassrooted Trust, Positive Hopes Alliance, Lanka Plus, National Union of Seafarers in Sri Lanka (NUSS), National Union of Metal & Migrant Workers in Sri Lanka and volunteers. It includes Lankans of diverse sexual orientation and gender identity, medical and legal professionals.

Phase one of bakamoono.lk focused on HIV, based on the need of the hour for citizens in Sri Lanka to have access to scientifically accurate and comprehensive information on modes of transmission, prevention, and also, support. It also looked at sex and relationships, which includes information on consent, gender, cyber exploitation, violence and available government and non-government services to support us and help us through difficult times.

Bakamoono.lk is a scientifically based and empathy driven effort to ask and answer taboo questions in Lankan society, and to promote conversations on these key issues.

Read more: http://www.bakamoono.lk/en

CASE STUDY 5: #MeToo

One of the most prominent recent examples is the role social media has played in highlighting the “Me Too” movement around sexual harassment and assault. It illustrates how a single social media post can resonate with so many and go ‘viral’ with global reach.

On 15 October 2017 when American actress, producer, activist and former singer Alyssa Milano took to Twitter posting the tweet: “If you’ve been sexually harassed or assaulted, write ‘me too’ as a reply to this tweet.” She emphasized that the basis of her hashtag was to create a platform where women had an "opportunity without having to go into detail about their stories if they did not want to".

The response was overwhelming. Within 24 hours, her post generated thousands of replies, comments and retweets -- and inspired thousands more original posts on social media, with women and men from around the world sharing personal stories. Milano wasn’t surprised to learn that so many people had #MeToo stories — but she was surprised about how candid they were in telling those stories on social media.

Me Too as a social movement began a decade earlier with Tarana Burke, a civil rights activist from the Bronx in New York. In 2006, Burke began using the phrase “Me Too” to raise awareness of the pervasiveness of sexual abuse and assault in society, and the phrase developed into a broader movement, following the 2017 use of #MeToo as a hashtag after the Hollywood producer Harvey Weinstein sexual abuse allegations and Milano’s tweet.

The virality of the “Me Too” movement briefly reached Sri Lankan social media spaces with dozens of women using the opportunity to share their experiences, but saw greater success in countries like India where people were named and shamed and as a result, and faced real consequences.

[If you are a resident in Sri Lanka and would like to speak to someone about sexual harassment or assault you faced or are facing, please reach out to Women In Need via their website or call them on 011 4718585.]

Read more: https://metoomvmt.org/about/
https://www.vox.com/identities/2018/10/9/17933746/me-too-movement-metoo-brett-kavanaugh-weinstein
https://www.bbc.com/news/world-asia-india-47025662

DISCUSSION POINTS

Here are a few questions and discussion points for further exploring this topic.

- What made Mahatma Gandhi one of the most effective political activists in history? How did his nonviolent activism influence other giants like Martin Luther King Jr., and Nelson Mandela?

- Why is offline activism still needed, especially in countries like Sri Lanka? Why can't all activism and advocacy be done just in social media?

- Besides memes, hashtags and online petitions, which other tools or strategies can be useful for digital activism?

- Can you name more local or national level examples of digital activism that have created impact at some level in recent years?

- Are you aware of a civil society organization or advocacy group that successfully combines online and offline methods in their social change campaigns?

- Have you ever initiated or signed an online petition? If so, discuss on what issue or topic, and its final outcome.

- One criticism of digital activism is that the action may have little effect other than to make the person doing it feel satisfied that they have contributed – this is called slacktivism. Do you agree? Discuss.

- The #MeToo movement started in the West but soon spread to other parts of the world, empowering women who have been sexually harassed or abused to talk about it and even name their perpetrators. #MeToo came to India, but not quite to Sri Lanka. Why do you think it has not happened in Sri Lanka yet (as at mid-2019)?

LEARNING OUTCOMES

By the end of this module, you will have an understanding of the following:

- Activism is more than agitation. The most effective activists analyze problems, listen widely and identify solutions that they advocate through different methods.
- Good public communication is a key part of activism. As technology advanced, more communications tools have become available for activism: the printing press, radio, television, web and social media among them.
- Digital activism, also known as cyber activism, is a form of activism that uses the internet and digital technologies as key tools for awareness raising, mobilization and action.
- For any kind of activism to become effective, it is essential to understand the country's social, political and cultural realities. For this reason, global campaigns need to be localized.
- For those engaged in digital activism, there are various strategies and tools – such as hashtags, memes and online petitions – with which to build virtual communities and to engage in dialogue.
- Two-way communication is an essential quality of online campaigns and advocacy: activists need to regularly engage supporters as well as those who might be curious or critical.
- There is a growing number of social, humanitarian and political reform campaigns that have been promoted through digital activism in Sri Lanka. Not all have been equally effective, and that holds valuable lessons for all who are keen to enter digital activism.

FURTHER READING

Freedom on the Net 2018 Sri Lanka report
https://freedomhouse.org/report/freedom-net/2018/sri-lanka

Activism in the Social Media age
https://www.pewinternet.org/2018/07/11/activism-in-the-social-media-age/

Activism on Social Media: A Curated Guide
https://ourdataourselves.tacticaltech.org/posts/23_guide_social_media/

Digital Activism Decoded: The New Mechanics of Change
https://www.opensocietyfoundations.org/publications/digital-activism-decoded-new-mechanics-change

The man behind Avaaz: Can we change the world, one click at a time? Ricken Patel, a young Canadian, thinks so. 1843 Magazine, May/June 2013.
https://www.1843magazine.com/content/features/robert-butler/man-behind-avaaz

Visualising Information for Advocacy, 2013 book by Tactical Technology Collective
https://visualisingadvocacy.org/

New Tactics in Human Rights website's guide to visualization information
https://www.newtactics.org/conversation/visualizing-information-advocacy

Ethics in Online Activism: False Senses of Social Action or Effective Source of Change?
Fordham University Center for Ethics Education, 2016.
https://ethicsandsociety.org/2016/02/17/ethics-in-online-activism-false-senses-of-social-action-or-effective-source-of-change/

Was Kony 2012 Social Media Activism or Mere Slacktivism?
Media Ethics Initiative
https://mediaethicsinitiative.org/2019/02/27/the-ethics-of-online-activism/