SCHOOL OF COMMUNITY NETWORK LEARNING SERIES

2026

INTERNET AND DIGITAL SAFETY

SCHOOL OF COMMUNITY NETWORK LEARNING SERIES

2026

Internet And Digital Safety

COMMONROOM NETWORKS FOUNDATION www.commonroom.info

ISEA Institute for Social Entrepreneurship in Asia

Foreign, Commonwealth & Development Office

RHIZOMATICA

APC

Publication Credits (Indonesia)

Programme Coordinator	Gustaff H. Iskandar
Chief Editor	Tisha Anwar
Administration	Reina Wulansari, Daffa Naufal, Sara Verawati
Ilustrasi	Sam & Ridha Kelana

Contributing Institutions

ICT Watch Indonesia	Heru Tjatur, Donny B.U., and Mataharitimoer
Relawan TIK	Fajar Eri Diyanto
APJII	Andri Aslan
Institut Teknologi Garut (ITG)	Ade Sutedi, Adi Susetyaningsih, Andri Ikhwana, Dedi Sadudin Taptajani, Dewi Rahmawati, Dewi Tresnawati, R. Dini Destiani Siti F., Eko Walujodjati, Leni Fitriani, Ridwan Setiawan, Muhammad Rikza N., and Rinda Cahyana
PokdarTIK	Erni Sulistyowati
Phytonesia	Andri Johandri
Bitread	Auliya Millatina Fajwah, Anita Khairunnisa, Acep Zaelani, Nana Sukmana, and Nakita Rizky Oktaviani

English Translation

Translation Project Coordinator	Akhmat Safrudin
Translator	Rudi Dwi Hartanto

Indonesia Publisher

Common Room Networks Foundation (Common Room)

Jl. Cigadung Asri I No. 3, Kel. Cigadung, Kec. Cibeunying Kaler, Kota Bandung, West Java 40191, Indonesia

Website: http://www.commonroom.info Email: email.commonroom@gmail.com

English Version is Published with The Support From
Association for Progressive Communications (APC)

Foreword

During the global COVID-19 pandemic, which began spreading across Indonesia in early 2020, internet infrastructure and services became an essential necessity — not only for daily communication, but for virtually every aspect of life: public services, long distance learning, healthcare, and pandemic response.

Although recent years have seen meaningful improvements in internet infrastructure and service coverage across Indonesia, the challenge of the digital divide remains a real and present problem, particularly for residents of rural and remote areas. This divide is driven by a complex combination of factors, including geographical constraints, insufficient infrastructure, limited device access, high bandwidth costs, inadequate digital skills and literacy, a shortage of local content, and persistent gender gaps in technology access. The School of Community Network Program (*Sekolah Internet Komunitas*) was established in Indonesia as a collaborative initiative to address these digital divide challenges. Developed jointly by Common Room and the Association for Progressive Communications (APC), and also supported by the Foreign, Commonwealth and Development Office (FCDO — UK), the programme involves ICT Watch, *Relawan TIK,* APJII, and the Garut Institute of Technology (ITG).

This book series forms part of the curriculum and training material framework to be developed within the School of Community Network Programme. The series encompasses ten thematic areas, from policy and regulation to foundational knowledge of computers and internet networks, and practical guidance on internet use for a variety of purposes. We sincerely hope that this guide will contribute to the long-term effort to overcome the digital divide in Indonesia and beyond through the translated module by building digital skills, knowledge, and literacy. especially among communities in rural and remote regions.

Bandung, December 2021

Gustaff H. Iskandar
Common Room Networks Foundation

Table of Contents

Publication Credits (Indonesia) *2*
Contributing Institutions 2
English Translation 2
Indonesia Publisher 2
Foreword *3*
Table of Contents *4*
DIGITAL LITERACY *6*
A. Healthy and Safe Online Socialising *8*
1. Social Media Networking 9
2. Basic Rules for Socialising Online 11
3. Platforms for Digital Expression 12
4. Freedom of Digital Expression 12
5. The Positive and Negative Dimensions of Digital Networking 13
B. Information Ethics and Intellectual Property *14*
C. Citizen Journalism *19*
1. Think Before Posting 19
2. Becoming a Credible Citizen Journalist 21
D. Individual Privacy Protection *22*
1. Limit the Personal Information You Share 23
2. Be Careful When Taking and Posting Selfies 24
3. Protecting Your Personal Digital Data 25
4. Be Cautious About Granting Application Permissions 27
A. Online Threats: How Serious Are They? *30*
1. Is the Digital World Truly Unsafe? 30
2. What Is Cybercrime? 31
3. The Most Common Forms of Cybercrime 32
a. Spam 32
b. Malware 32
c. Spyware 32
d. Phishing 33

e. Hacking 33
4. How to Protect Yourself from Online Threats 34
B. Hoaxes *35*
1. Recognising Hoaxes 37
C. Cyberbullying *43*
1. Why Does Cyberbullying Occur? 43
2. Where Can Cyberbullying Occur? 44
3. Who Are the Victims of Cyberbullying? 45
4. Responding to Cyberbullying 45
References *48*

CHAPTER

01

DIGITAL LITERACY

In this chapter, you will hopefully learn:

✓ Define digital literacy and explain why it matters for everyday internet users.

✓ Describe the principles of healthy and safe online socialising on social media.

✓ Explain what information ethics and intellectual property mean in a digital context.

✓ Understand the concept of net journalism and the responsibilities of online information sharing.

✓ Identify ways to protect individual privacy and personal data in digital environments.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

☐	Basic familiarity with social media platforms (Facebook, Instagram, or similar).
☐	General understanding of what the internet is and how it is accessed.
☐	No prior technical knowledge is required for this chapter.

“DIGITAL LITERACY”

What comes to your mind when you hear the word ‘literacy’?

If your answer involves reading and writing, you are not wrong. Literacy has traditionally referred to an individual’s ability to read and write. However, literacy can be understood more broadly: it describes the knowledge, skills, and abilities required to process information in a specific field or activity. It is not limited to reading and writing.



Figure 1 Smartphone Adapation starts early, digital literacy is a necessity in each and every member of the family

Photo by Justin Severus on Unsplash

Digital literacy is the ability and knowledge required to use digital technology and media wisely, with the aim of fostering positive communication and interaction.

If you understand the importance of digital literacy, you will be empowered to become a smart technology user. When receiving information from the media, you will be able to interpret it critically and wisely. You will also be able to filter what you receive, so that you do not fall prey to misinformation and hoaxes.

Digital literacy makes you more discerning when it comes to seeking, filtering, receiving, and sharing information.

A. Safe Online Socialising

Online Social Network Site have become the integral part of our live. Since the early 2000s to around 2002, This trend has grown immensely. Alongside the emergence of social networking sites such as Facebook, Instagram, Twitter, etc.

Safety for the future generation remain a pressing issue, Both Children and adults are equally present online. Whether it's for online learning, social networks, blogs and vlogs, or online meetings. As more devices connect to the internet, access to the online world has become easier than ever. The emergence of Facebook Pro for example have created various communities based on location and interest.

Networking online is now entirely ordinary. We can socialise with hundreds, even millions, of people worldwide without ever meeting face to face. We can share information and experiences, inspiring, educating, or entertaining one another. However, certain limits must be observed to keep our online interactions healthy.

1. Social Media Networking

Social media is a familiar term, used not only for networking but also for promoting businesses. According to global digital reports analyzing screen time, the Philippines has almost 70 million smartphone users who spend nearly a third of their day (32.53%) on their phones. In contrast, while China has nearly a billion people, its average phone screen time sits much lower at 19.54% due to platform restrictions. This heavy digital engagement means Filipinos spend over one-fifth of their day (21.91%) specifically on social media platforms—ranking among the highest globally.

Internet users in the Philippines are predominantly from Generation Y (Millennials) and Generation Z, groups that have grown up alongside smartphones, computers, and the internet.

When being used with good intention and wisely, social media allows you to collaborate and maintain continuous communication with those around you, regardless of distance. If you run a business, social media enables active and engaging interaction with potential customers. Rather than simply posting selfies, consider sharing knowledge and insights related to your field. Networking on social media is about more than making acquaintances, it is an opportunity to share knowledge and do good. Sharing is caring.



Figure 2 *Even though children don't play on social media, parents, not just school still play an important role in monitoring their digital habits through guidance.*

Photo by Justin Severus on Unsplash

2. Basic Rules for Socialising Online

Socialising in the digital world comes with rules, just as it does in real life. Each platform or website has its own privacy policy that users must follow. Although these policies can be lengthy, reading them carefully allows you to understand your rights and obligations.

The following are fundamental rules to observe when socialising online:

- Do not create accounts using someone else's identity. Be yourself and avoid misrepresenting yourself to others.
- Always credit the source when sharing content created by others. This constitutes proper recognition of intellectual property.
- Do not post inappropriate photographs, as these can be misused and cause harm.
- Do not spread messages in hate speech tone or misinformation (hoaxes). Both have the potential to divide communities, and digital footprints are permanent.

Be thoughtful in choosing your words when leaving a comment, and make a habit of filtering information before you share it. Think before posting!

3. Platforms for Digital Expression

In this digital era, we benefit from increasingly fast and stable internet connections, and from the growing number of platforms available for self-expression. The most widely used social media platforms globally include Facebook, YouTube,Instagram, Twitter, WhatsApp, TikTok, Line, LinkedIn, Telegram, and Pinterest. And there are forums such as Reddit and interest based forum on Facebook Groups.

For expressing opinions, blogging platforms such as Tumblr, Blogspot, and WordPress were used to be popular, but nowadays platform such as Substack, Medium have also emerged as spot to share opinions.

The important thing is to be wise and choose which Social Network you deem as necessary and which one is just for filling up free time. Choose a few that suit you and support how you wish to express yourself. If you enjoy watching video content, the rise of TikTok and YouTube make those natural choice. For communication and keeping up with close friends, you might select a messaging platform such as WhatsApp or Telegram. Quality matters more than quantity.

4. Freedom of Digital Expression

> *Freedom of expression is the right to express ideas and opinions freely, through speech, writing, or other means, without infringing upon the rights of others.*

In the digital world, you can exercise your freedom of expression by posting statuses, captions, photos, and videos on social media. However, freedom of expression does not mean freedom to spread false information, slander, hate speech, or content that touches on ethnicity, religion, race, or inter-group relation. Everything posted online is recorded and accessible to many people. Act responsibly.

5. The Positive and Negative Dimensions of Digital Networking

The digital world is like a double-edged sword. Used for positive purposes, it can be a platform for learning, build relationships, and growing a business. Used carelessly or with harmful intent, it can inflict real damage, including through cyberbullying and online fraud.

Positive Impacts	Building networks with people around the world; a vehicle for personal development; proving that distance does not prevent us from showing care and empathy.
Negative Impacts	Over-reliance on gadgets; reluctance to communicate face to face; impaired language comprehension; excessive time spent online at the expense of one's immediate environment; a fertile ground for predatory criminal activity.

B. Information Ethics and Intellectual Property

Information ethics is the awareness required to evaluate issues related to the dissemination of electronic data.

Intellectual property belongs to its creator. Creators have the right to recognition and appreciation, and to protection from misuse. This is why it is essential to apply information ethics when sharing content online. Types of intellectual property protection include copyright, copyleft, patents, Creative Commons licences, trademarks, and attribution of credit.

By understanding information ethics, you will no longer fall for hoaxes, because you will be able to filter what you receive. You will also be better equipped to evaluate and communicate information appropriately, and to respect the creative work of others.

Becoming a Digital Content Creator: Text, Video, and Beyond

Intellectual property belongs to its creator. Creators have the right to recognition and appreciation, and to protection from misuse. This is why it is essential to apply information ethics when sharing content online. Types of intellectual property protection include copyright,

copyleft, patents, Creative Commons licences, trademarks, and attribution of credit.

By understanding information ethics, you will no longer fall for hoaxes, because you will be able to filter what you receive. You will also be better equipped to evaluate and communicate information appropriately, and to respect the creative work of others.

1. Choosing Your Platform and Format

The landscape of content creation has expanded far beyond the traditional blog. Today, creators can choose platforms that best match their voice, skills, and audience. The main formats are:

Written / Long-form Text Medium is a publishing platform where you write articles and essays for an existing reading community. It handles distribution built-in — your work can reach readers who don't already follow you. Substack is a newsletter platform where readers subscribe directly to you, not to a feed. It's especially powerful for building a loyal, direct-to-inbox audience and can be monetised through paid subscriptions from day one. Both are far more discoverable and community-connected than a standalone blog, though maintaining your own website remains useful for a professional portfolio or SEO-driven content.

Short-form Text and Thought Leadership Platforms like X (Twitter), Threads, and LinkedIn reward consistent, punchy writing. X and Threads favour real-time commentary, hot takes, and building in

public. LinkedIn is stronger for professional positioning and B2B audiences. Short-form writing teaches you to communicate ideas economically—a skill that strengthens all your other content.

YouTube remains the dominant long-form video platform and functions as a search engine in its own right—content published there can surface for years. TikTok and Instagram Reels favour short, high-engagement vertical video and can grow an audience rapidly. YouTube Shorts bridges both worlds. Each platform has distinct editing norms, pacing expectations, and audience demographics—study the format before committing.

Benefits of content creation regardless of format include: sharpening communication skills; fostering creativity and original thinking; generating income through monetisation; building and expanding your network; expressing ideas and positioning yourself as a subject-matter voice; and developing a practical understanding of how digital platforms and algorithms work.

2. How to Grow Your Audience

Regardless of the quality of your content, without a network and without applying the right techniques, your content will remain undiscovered. The following approaches work across formats:

Consistency over frequency. Showing up reliably on a schedule — even if that means publishing less often — builds audience trust and trains the algorithm to surface your work.

Understand platform-specific SEO. On YouTube, titles, descriptions, tags, and thumbnails determine whether your video gets recommended. On Medium and Substack, clear headlines and topic tagging affect discoverability. On TikTok, audio trends, hashtags, and watch-time in the first three seconds matter most. Each platform rewards those who learn its logic.

Cross-promote across channels. A single idea can become a Substack essay, a LinkedIn post summarising the key argument, a short video breaking it down on TikTok or Reels, and a thread on X. Repurposing content multiplies your reach without multiplying your workload.

Engage, don't just broadcast. Comment meaningfully on other creators' content in your niche. On Substack, recommend other newsletters and they may reciprocate. On YouTube, respond to every comment in the early stages — the algorithm reads engagement as a signal of quality.

Collaborate and cross-pollinate. Appear as a guest on someone else's podcast, write a guest essay for another Substack, or do a collab video. This introduces you to an established audience that already trusts the host.

Build a community around your content. Join or create a Discord server, Telegram group, Facebook Group, or Substack Chat where your audience can engage with each other — not just with you.

Communities with genuine peer interaction retain audiences far better than passive follower counts.

Use calls to action. Ask readers to subscribe, share, or comment. On Substack, ask them to recommend your newsletter to one person. These small nudges have a significant compounding effect over time.

3.What May and May Not Be Shared

In content creation, it is nearly impossible to produce work in a complete vacuum — you will draw on existing sources, respond to others' ideas, and use images, data, or quotes to support your points. When quoting text or using images, illustrations, data, or audio created by others, always credit the original creator clearly. Where possible, seek permission from the copyright holder before reproducing or distributing their work. Use Creative Commons-licensed material where you cannot obtain permission, and always link back to the original source.

Avoid plagiarism and copyright infringement — both damage your credibility as a creator and can result in content removal, demonetisation, or legal action on commercial platforms. When using AI tools to assist your writing or video production, be transparent with your audience about how you use them. AI-assisted content is increasingly common, but audiences value authenticity; your original perspective and voice are what build lasting trust and loyalty — not the tools you use to produce it.

C. Citizen Journalism

Citizen journalism is the form of citizen participation in disseminating information and news through various online applications and channels.

Citizen journalism is necessary to support and complement mass media. Because of limited personnel or remote locations, professional journalists cannot always be present at every incident. Citizen journalism fills this gap by recording and reporting events as they happen, without any particular agenda. The rise of local based account reporting on what is happening in local scope is also hlping information distribution

However, 'reporting as it happens' does not mean that citizens may post anything without filtering. On the contrary, internet users must exercise careful judgement, since the information they share may affect the lives of other people.

1. Think Before Posting

Social media has become the primary platform for information distribution. People tend to search for and share information through social media because it spreads quickly and 'can go viral'. If used unwisely, however, social media can become fertile ground for prohibited content, hate speech, hoaxes, and cyberbullying. The old Indonesian proverb 'your mouth is your tiger' has shifted in the digital age to 'your status is your tiger'.

Before posting anything, ask yourself: Will this hurt someone? Could it constitute defamation? Does it contain negative content? Is it true, or is it a hoax? The dissemination of information in digital form is governed in Indonesia by Law No. 11 of 2008 on Electronic Information and Transactions (the ITE Law). Violations carry legal consequences.

Check and recheck every item of news you receive, then consider carefully whether it is important enough to pass on.

When sharing information or news, always present factual, current, and accurate content without embellishment or omission. The key requirement is neutrality, do not take sides or attempt to steer public opinion. The same applies to comments and replies: think carefully before posting, and ensure that what you say does not constitute hate speech, defamation, or content that offends any individual or group.

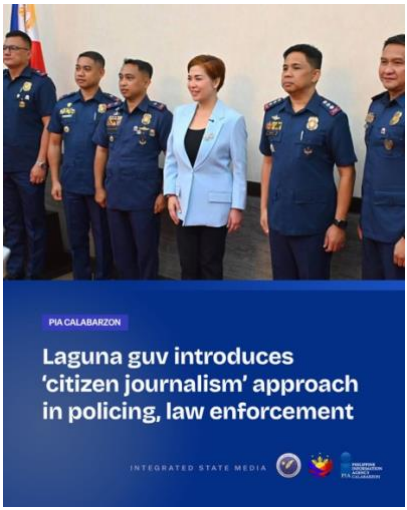


Figure 3 Laguna guv Citizen Journalism aim to help local government in law enforcement.

2. Becoming a Credible Citizen Journalist

Even as a net journalist, you must be responsible for what you publish. A digital footprint is created the moment you post anything. Once you post, even if you delete it, the record remains, other users may have already saved or shared your content. Therefore, commit to being a credible net journalist.

Steps to follow before publishing information online:

1. Collect all information based on available facts.
2. Validate the information you have gathered.
3. Where possible, supplement with supporting data (photos, video, statistics, interviews).
4. Summarise all the information.

5. Do not reduce or exaggerate the information.
6. Publish on social media or an online news channel.

D. Individual Privacy Protection



MANILA BULLETIN

Philippines World Business Opinion Lifestyle Entertainment Sports MB126

ADVERTISEMENT

Technews

ASEAN Foundation launches 'Scam Ready ASEAN' in response to rising online scams in Southeast Asia

By Manila Bulletin Newsroom

Published Apr 30, 2026 10:27 am

The ASEAN Foundation launched Scam Ready ASEAN, a regional initiative aimed at strengthening prevention against online scams across Southeast Asia. The programme was unveiled at the Google 2026 Online Safety Dialogue in Kuala Lumpur earlier today, a forum bringing together policymakers, industry and safety experts focused on combatting the growing threat of online fraud and scams.

Supported by Google.org with USD 5 million funding, the programme aims to build scam resilience for 3,000,000 people across ASEAN, representing one of the region's largest-ever digital defence initiatives against online scams. Scam Ready ASEAN seeks to equip ASEAN communities with the knowledge, digital confidence, and critical thinking skills needed to recognise and prevent scams in an increasingly complex online environment.

Latest Stories

PNP probes into P13 M smuggled cigarettes seized in Lanao del Sur

Police rescue wildlife species from Cebu resort

Poverty, crime rates in Bohol drop

Figure 4 With the rise of online scam, personal data is now more important than ever before.

> *Personal data protection refers to the protection of data about a person's life that can be identified directly or indirectly — whether through electronic or non-electronic systems.*

Personal data must be protected because it underpins a person's ability to participate in many aspects of life: school enrolment, marriage, opening a bank account, applying for a credit card, registering for vaccination, and receiving social assistance. At the same time, much personal data is falling into irresponsible hands

and being used for criminal purposes, including credit card fraud, scams, and defamation.

As an individual, you have the right to control, edit, manage, and delete information about yourself to prevent it from entering the public domain. You also have the right to decide when, how, and to whom that information is disclosed. No party has the right to compel you to share personal information, including photographs of yourself.

Categories of individual private data include: home address, health history, phone number, parents' names, photographs, bank account numbers, and date of birth.

We sometimes unconsciously put private things such as an address without even noticing, it is important that we could double check everything before posting. Aside from posting making sure that we store our personal data in a secure password manager apps, or private notes is important to prevent the danger of storing our password on plain notes or personal chat.

1. Limit the Personal Information You Share

The protection of personal data has become a critical issue. Acts of theft involving personal information, not only credit card or bank account numbers, but also full names, email addresses, phone numbers, national ID numbers, or health records, all constitute criminal offences.

Data stored there included addresses, family registration cards, national ID numbers, salary information, and employer details. Such

data represents access to deeply personal aspects of a person's life. Through it, bank accounts can be compromised and personal data used for criminal purposes, such as registering for online loans.

2. Be Careful When Taking and Posting Selfies

Taking selfies and posting them on social media has become a common habit, particularly among Millennials. However, selfie photographs can be misused. In some cases, selfies have been used to facilitate money-lending fraud. In others, photographs have been edited, often in a sexually explicit manner, and then published online. To protect yourself, observe the following principles:

- Avoid poses that lean toward pornographic content, or that could be misinterpreted. Remember that anything you post on social media automatically becomes public and can be saved or misused.
- Do not put yourself in physical danger for the sake of a photo. Numerous reports exist of selfie-related accidents. Take selfies only in safe and appropriate places.
- Exercise caution when making contact with strangers. Use social media's report function if you receive suspicious messages. Never arrange to meet someone you have only known online, and if it is unavoidable, do so in a public place and not alone.

Be careful when meeting someone for the first time online, as not everyone uses their real identity. Do not allow

yourself to be trapped or deceived by irresponsible individuals.

3. Protecting Your Personal Digital Data

Data breaches are not always large-scale events. They can also result from our own carelessness or lack of awareness, for example, when an application asks us to take a selfie alongside our national ID (PhilSys ID / PhilID) for verification.

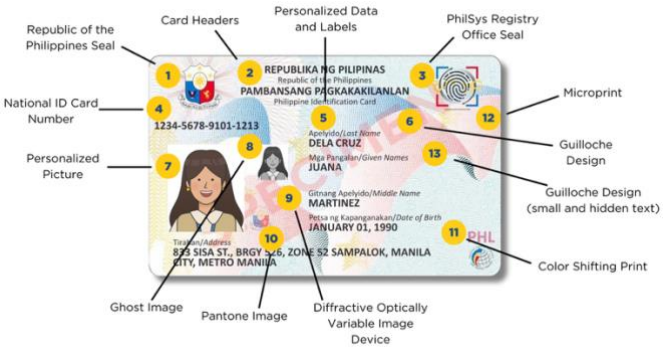


Figure 5 Have you got a digital copy of your Philippines ID?

Although this practice is now increasingly common across e-wallets, lending apps, and online services, it should be approached with caution. In many cases, what gets stolen is not only the physical card, but also a photo or scan of your ID combined with supporting details like your full name, birthday, address, and mobile number, a combination often sufficient to pass weak Know Your Customer

(KYC) checks. The PhilSys ID is one of the most important documents requiring protection. It can be used for a wide range of transactions: applying for social welfare and benefits; availing of services from SSS, GSIS, Pag-IBIG, and PhilHealth; applying for passports and driver's licenses; tax-related transactions; voter registration; opening bank accounts; job applications; and other transactions requiring proof of identity. This breadth makes it an especially high-value target for fraud and identity theft.

Under the Data Privacy Act of 2012 (Republic Act 10173), personal data is categorised into personal information, sensitive personal information, and privileged information, each carrying different levels of protection. Sensitive personal information includes data about your race, ethnic origin, marital status, age, religious or political affiliations; your health, education, genetics, or sexual life; and government-issued identifiers unique to you, such as your Social Security System (SSS) number.

Beyond the PhilSys ID, several other documents and identifiers deserve particular vigilance in the Philippine context:

- PhilSys Number (PSN) — your unique lifetime identifier in the national ID system. Legislators have raised alarms that visible printed PSNs on ID cards are easily copied by fraudsters, with a 2024 incident where the PSA warned the public against unauthorized individuals photographing national IDs in exchange for cash.

- SSS / GSIS numbers — linked to your employment records, contributions, and loan eligibility
- TIN (Tax Identification Number) — used across financial and government transactions
- PhilHealth and Pag-IBIG numbers — tied to your benefits and housing loan records
- Voter's ID / COMELEC registration details
- GCash, Maya, and other e-wallet account credentials and OTP codes

Identity theft incidents in the Philippines are on the rise: 1,597 cases were reported in 2023, a 13.9% increase from the prior year, and over 315,000 identity credentials were compromised in just the first half of 2024.

4. Be Cautious About Granting Application Permissions

Be careful about the applications you download. If an application requests access to your contacts list or photo gallery, examine this carefully before granting permission. Is access to those resources genuinely necessary for the application's function?

Key steps to securing your personal digital data:

- Do not expose personal data in public spaces, whether online or offline. Avoid posting photos of your IDs or even your face in ways that could be combined with other data to identify you.

- Do not share personal data or specific codes (such as OTP codes sent by SMS or through GCash/Maya notifications) with others, especially if you did not initiate the registration or transaction.
- Do not lend your phone to strangers. If attackers gain control of your phone number, they can intercept OTPs and reset passwords on your accounts.
- Never tell others your PIN or password, including bank or e-wallet customer service agents.
- Be cautious of apps requesting a selfie-with-ID. Only share this with verified, legitimate platforms. Under Republic Act 11055, any person who collects or uses PhilSys personal data for purposes other than authentication or identity verification can face 6 to 10 years of imprisonment and fines of up to ₱5,000,000.
- Only download government apps like eGovPH from official stores (Google Play or Apple App Store). Downloading from unofficial sources increases vulnerability to fraud.
- Protect your personal data by setting privacy controls on your photo gallery and social media accounts.

CHAPTER

02

CYBERCRIME, HOAXES, AND CYBERBULLYING

In this chapter, you will hopefully learn:

✓ Explain what cybercrime is and identify its most common forms.

✓ Describe practical steps to protect yourself against spam, malware, spyware, phishing, and hacking.

✓ Define what a hoax is and explain how to recognise and prevent one from spreading.

✓ Explain what cyberbullying is, where and why it occurs, and how to respond appropriately.

✓ Describe the digital divide in Indonesia, including its gender dimension.

Prerequisite Checklist

Before proceeding, ensure you are comfortable with:

☐	Understanding of basic online socialising norms covered in Chapter 1.
☐	Familiarity with social media platforms and messaging applications.
☐	General awareness of what viruses or harmful software are.

Although the digital world now touches virtually every aspect of life, many internet users are relatively passive when receiving information, unable to filter the importance and unable to or critically analyse it. As a result, unverified information spreads rapidly, reaching all segments of society and giving rise to a range of responses and assumptions. Unverified information can steer public opinion and mislead people.

Make it a habit to examine and validate any information you receive before passing it on.

A. Online Threats: How Serious Are They?

Threats exist in both the physical and the digital world. Neither can be ranked as simply 'more serious' than the other, the gravity of a threat depends on its context. Threats in the digital world should never be underestimated: the domino effect they produce can be severe.

1. Is the Digital World Truly Unsafe?

The internet has transformed the way people live, work, communicate, and shop. Digital communication, email and social networking, is now considered more efficient and effective than many traditional forms.

However, the internet is also a source of concern: negative content, including pornography, online gambling, fraud, harassment, defamation, and cyberbullying against children and teenagers, is

widely reported. Cybercrime, including the hacking of critical national websites, occurs with considerable frequency.

Despite these risks, interaction with the digital world is unavoidable. The only available course of action is to act wisely when accessing the internet, thereby minimising the threats involved. This requires internalising and practising the principles of safe and healthy internet use (cyber ethics) from an early age.

Whether the digital world is safe depends, to a significant degree, on the security precautions you apply. If you are careless about privacy and access, threats will be more likely to affect you. The digital world is closely associated with anonymity, making threats and their perpetrators more difficult to trace than in the physical world.

2. What Is Cybercrime?

> *Cybercrime is criminal activity carried out in the digital world through the use of computer technology and internet networks.*

Since the COVID-19 pandemic struck Indonesia, many people have lost their livelihoods. This has been one of the factors driving an increase in criminal activity—not only physical crime, but also cybercrime, in a growing variety of forms ranging from fake fundraising on behalf of pandemic victims, to data theft and bank account fraud.

Cybercrime typically targets devices, hardware, software, and personal data. It tends to be more complex and harder to address than physical crime, because both perpetrator and victim are invisible to each other. Perpetrators can conceal their identities through anonymity and can destroy evidence. It is often impossible to determine whether a perpetrator is an individual or a group.

3. The Most Common Forms of Cybercrime

a. Spam

Spam refers to unsolicited bulk email arriving in a user's inbox without their request. Its content varies: product or service offers, fraudulent business propositions, multi-level marketing schemes, or unwanted advertising. Spam is a serious security concern: it can be used to deliver trojans, viruses, worms, spyware, and phishing content. Ignore spam from unrecognised senders.

b. Malware

Malware is software containing malicious code, such as viruses, worms, and trojans. It spreads through popular communication media including email, instant messaging, websites, and peer-to-peer download connections. Malware also attempts to exploit vulnerabilities in the operating system. Once a device is infected, data can be damaged or destroyed.

c. Spyware

Spyware is a malicious programme that hides within a computer. True to its name, it monitors all the activities you carry out on the

internet and then steals important data — usernames, passwords, and bank account information — sending it to its creator. Spyware typically installs itself automatically when you download illegal software, click on advertisements on certain websites, or click on links in emails or instant messages.

d. Phishing

Among all forms of cybercrime, phishing is arguably the most frequently encountered. This type of online fraud aims to steal victims' important data, such as usernames, passwords, and credit card details. Perpetrators typically exploit current events — natural disasters, competitions, e-commerce, or social media verification — as social engineering hooks. Victims are usually sent a link leading to a fake website, where they are asked to enter their username and password or to sign up by providing personal information.

e. Hacking

Hacking is the direct targeting of a victim's computer system or network, enabling the hacker to enter the system and take control. The term itself is neutral, but hacking is widely used by cybercriminals. This form of cybercrime is arguably the most dangerous, because the victim cannot easily avoid or anticipate it in the same way as with spam or phishing. Large volumes of sensitive data can be leaked. The only preventive measure available is to tighten computer security.

4. How to Protect Yourself from Online Threats

General precautions applicable to all forms of online threat:

- Always scan for virus on your device with included security software in your smartphone.
- Software on your computer and smartphone.
- Use strong passwords combining letters, numbers, and special characters.
- Be selective about the applications you download.
- Avoid clicking ‘agree’ on websites or applications without reading the terms and conditions.
- Always keep your browser and software up to date.
- Back up your data regularly, in more than one location.

Specific precautions by threat type:

Spam	Ignore spam rather than clicking ‘unsubscribe’ (which confirms your address is active). Never click links in emails from unknown senders. Activate the anti-spam feature in your email client.
Malware	Back up your computer data regularly. Never open attachments or links from unknown sources in email, social media, or instant messages. Scan files with antivirus software before opening. Always update your browser and security patches.

Spyware	Be selective about what you download. Read software licensing agreements carefully before installation. Scan your computer regularly. Be cautious of pop-up advertisements.
Phishing	Never click on suspicious links. Do not provide personal information to unknown parties. Note that banks will never ask for your PIN or password. Ensure that websites you visit use ‘https’ (indicated by a padlock icon).

B. Hoaxes



Figure 6 FB Post Containing False Post

source: personal documentation

> *A hoax is a false or unsourced piece of news presented as genuine, with the aim of misleading readers or distorting the facts.*

It must be acknowledged that hoaxes today are increasingly well-packaged, and many readers believe them. They spread rapidly and, like a snowball, the ‘falsehood’ in their content tends to grow

larger over time. Common subjects for hoaxes include religion, politics, health, business, natural disasters, and road traffic.

Hoaxes typically exploit the good intentions of readers, who quickly share what they consider 'important' news without first verifying its accuracy. In addressing this, we must prioritise validation above all else. Do not allow yourself to be misled by hoaxes.

1. Recognising Hoaxes

The following characteristics can help you identify hoax information:

- The information is typically disseminated through social media or group instant messaging chats, for maximum speed and reach.
- The content tends to generate anxiety or panic in the reader.
- The information is entirely fabricated or is a distorted version of a genuine original.
- There is no connection between the title, images, and supporting content.
- The information and images have been manipulated.
- The piece usually concludes with an appeal to readers to spread it as widely as possible.

2. Where Is Disinformation Found

Disinformation is most commonly found on social media and through instant messaging apps. In the Philippines, Filipinos most commonly encounter disinformation on social media rather than on messaging apps, search engines, or through face-to-face conversation.

Facebook leads as the primary platform at 68%—well above the global average—followed by TikTok at 48% and YouTube at 39%. Through these platforms, false content spreads extremely fast and is easily shared, with readers adding their own reactions and comments that amplify its reach.

Through messaging apps like WhatsApp and Messenger group chats, people tend to forward content to multiple groups simultaneously. In both cases, the goal is the same: to reach as many people as possible and mislead as many readers as possible.

Common formats used to spread disinformation in the Philippine context include narratives that exaggerate, sensationalise, or provoke; images and photographs that have no connection to the content or have been edited; memes used as political commentary that blur the line between satire and fact; and increasingly, AI-generated and deepfake video content designed to appear authentic.

The New Threat: Deepfakes and AI-Generated Content

We are now in an era where seeing something in video form is no longer sufficient proof that it is real. AI-powered deepfakes are hyper-realistic synthetic media capable of imitating a person's likeness—combining images, audio, and video to create footage depicting events, statements, or actions that never actually happened. This is no longer a distant or abstract risk for Filipinos. During the lead-up to the 2025 midterm elections, the Cybercrime

Investigation and Coordination Center (CICC) reported between 200 and 300 deepfake incidents per day in March 2025 alone. In 2023, the Philippines already experienced the highest rate of malicious deepfake incidents in the Asia-Pacific at 4,500%, compared to a regional average of 1,530%.

Deepfakes have been used to fabricate endorsements, fake rallies, and produce misleading campaign videos that are difficult for the public to verify. In a recent example that sparked national debate, allies of Vice President Sara Duterte shared a viral video of AI-generated characters, presented as schoolboys and an elderly woman—to argue political points around her impeachment trial. The video was quickly exposed as a deepfake, yet the officials who shared it defended doing so. This illustrates a dangerous new norm: disinformation through AI-generated video can come from public figures themselves, not only anonymous trolls.

A fake "TV Patrol" newscast about a purported 2028 election survey also circulated on TikTok, using AI-manipulated images and voices of a real news anchor, reporter, and political analyst. If you encounter a video of a public figure saying something shocking or unexpected, pause before sharing—treat it with the same scepticism you would apply to an anonymous text message.

3. Sharing Information Wisely

When you receive information—in any format—always validate it before passing it on. Ask yourself: is this true? If yes, is it beneficial to share? Only proceed if both answers are affirmative.

The following guidance can help you examine and validate information:

a. Provocation in Headlines and Thumbnails

Disinformation is typically framed with provocative headlines or video thumbnails designed to trigger an emotional reaction before you think critically. When you encounter one, read or watch the full content.

Does it match what the headline or thumbnail claimed? Is it factual? Is it a genuine statement from an official source that may have been clipped out of context? Validate before deciding whether to share. Never comment on or share content after seeing only the headline or a few seconds of a video.

b. Check the Source

When you receive information, the first critical step is to verify the source. Where does it come from? Is the outlet or account verified and credible? In the Philippine context, be especially cautious of pages and channels that mimic the visual style of legitimate news organisations—using similar logos, fonts, and "breaking news" banners to give the impression of credibility. This type of content has

been described as "news cycle disinformation"—propaganda that camouflages as journalism, blurring the lines between professional reporting and attention-hacking. If the source is unknown or unidentifiable, disregard the information. Do not trust it, and do not share it.

c. Verify Photographs and Videos

Information that circulates is frequently accompanied by photographs or videos as supporting evidence. Not all such visuals are authentic or relevant. A photograph may be genuine but completely unrelated to the story it is being used to support. When in doubt, use a reverse image search (available on Google and TinEye) to check the origin of a photograph.

For videos, be especially careful. Ask: Is this from a verified official channel? Does the person's mouth movement match the audio naturally?

Are there signs of visual inconsistency around the face, hair, or background? AI-generated content often has subtle tells: unnatural blinking, slightly distorted hands, or audio that sounds just slightly, talking cat and unnatural poses, be on alert when facing video with unfamiliar color scheme?.

4. Sharing Information Wisely

The following steps can help you prevent and halt the spread of disinformation:

- Check whether the news or video you have received is accurate by tracing it back to its original source—an official website, verified account, or established news outlet.
- Only trust sources that are competent and of established credibility. Be aware that even public officials can share AI-generated disinformation.
- Consider whether the content triggers a strong emotional reaction—outrage, fear, or excessive patriotism. These are often engineered responses. Pause and verify before sharing.
- Ensure the information does not contain hate speech, false claims, or content targeting specific individuals or communities.
- Treat viral videos with the same critical eye as viral text. If a video shows a public figure saying something extraordinary, look for corroborating coverage from established outlets before believing or sharing it.

Tools and channels for reporting and fact-checking in the Philippines:

- Filipinos can turn to fact-checking sites including Rappler Factcheck Tsek.ph and its partners—VERA Files, ABS-CBN News, FactRakers, and Philstar—for verified information on circulating claims. VERA Files also operates

a Messenger-based tipline where users can submit suspicious content for fact-checking.

C. Cyberbullying

> *Cyberbullying is bullying that uses digital technology, carried out by an individual or group, repeatedly, against someone considered unlikely to be able to defend themselves. — UNICEF (unicef.org, 2020)*

Social media users are increasing every day, supported by the constant emergence of new platforms with ever more comprehensive features. Although social media is predominantly used by tech-savvy young people, it is frequently also used to spread bullying and hate speech.

Bullying is not a new issue in Indonesia. It has been a persistent problem for a long time, with victims ranging from children to adults. Children and adolescents tend to be the primary targets, particularly in school settings. As society has entered the digital era, bullying has not diminished—on the contrary, it has intensified. Online anonymity makes cyberbullying feel more 'intense', allowing perpetrators to direct verbal and visual harassment at victims without fear of being identified or reported.

1. Why Does Cyberbullying Occur?

The rapid development of technology — which allows users unrestricted access to all kinds of content — creates the conditions for cyberbullying. When users encounter content that does not align

with their views, they tend to leave comments expressing their disapproval, which can escalate into harassment. Cyberbullying can also stem from imitation: when someone directs intimidation at a target and it goes viral, others may follow, often without understanding the legal risks involved. Many young people do not yet realise that bullying can be reported and prosecuted.

2. Where Can Cyberbullying Occur?

Cyberbullying can occur across a wide range of platforms, including SMS, email, instant messaging (IM), blogs, social media, and online gaming platforms. Its forms include:

- Spreading false rumours.
- Posting embarrassing photographs.
- Verbal harassment.
- Excluding or isolating a child in online games.
- Spreading negative comments, threats, and intimidation.
- Creating group chats to spread hatred against a specific person.
- Creating fake accounts, hacking, or stealing someone's online identity to embarrass them.

Physical bullying and cyberbullying often occur simultaneously. Cyberbullying always leaves a digital trail, even when carried out anonymously. In cases documented internationally, some victims of cyberbullying who suffered severe psychological pressure and depression chose to end their lives. For this reason, let us look out for one another by preventing and avoiding cyberbullying.

3. Who Are the Victims of Cyberbullying?

Anyone can become a victim of cyberbullying, from primary school pupils to prominent public figures. Bullying tends to be directed at those perceived as weaker or unlikely to retaliate, as well as those considered to have physical or social shortcomings. Children and adolescents are the primary victims.

According to UNICEF (2016), between 41 and 50 percent of Indonesian adolescents aged 13 to 15 have experienced cyberbullying—including doxing (publishing others' personal data), cyber-stalking (online stalking that extends into the physical world), and revenge pornography (sharing intimate images for the purpose of revenge, accompanied by intimidation and blackmail).

Victims of cyberbullying sometimes do not report what has happened to them. It is therefore the responsibility of those around them to identify the signs. Indicators that a child may be a victim include:

- Sudden and excessive anger or distress after using the internet.
- Declining school grades or sudden avoidance of class or school.
- Signs of depression.

4. Responding to Cyberbullying

Because cyberbullying takes place online, it can attract unwanted attention from a wide audience, including strangers unknown to the victim. Some comments from other users may help the victim, while

others may further isolate and corner them. As a result, the victim can feel unsafe — as though under attack from all sides, even within their own home.

Something is a joke when people are 'laughing with you'. But if they are 'laughing at you' and you feel hurt, it may be bullying.

Cyberbullying must be stopped. When you encounter it, do not be indifferent. The following steps can help break the cycle of harassment and support victims:

- Reassure the victim that it is not their fault.
- Ask the victim not to respond, as cyberbullies always wait for a reaction. When the victim responds, the perpetrator feels validated.
- Do not retaliate or reply with equally negative comments.
- Save or print evidence of the cyberbullying.
- Identify the perpetrator.
- Ask the perpetrator to stop, and warn them that legal action will be taken if the behaviour continues.
- If the cyberbullying has escalated to violence, extortion, or sexual harassment, contact the police immediately.

Stopping cyberbullying is not just about exposing the bully. It is about affirming that everyone has the right to be respected

— in the digital world and in the real world alike. Let us protect victims and prevent new ones from emerging.

References

AlterMidya & WITNESS. (2025, May 9). *AI disinformation and the 2025 Philippine elections: Generative AI and deepfakes as tools of political repression*. WITNESS Media Lab. https://blog.witness.org/2025/05/generative-ai-philippine-elections2025/

BU, Donny and Eddy Prayitno (eds.). (2018). Media Sosial untuk Advokasi Publik [Social Media for Public Advocacy]. E-book. ICT Watch.

Cambridge Core / Data & Policy. (2025). Disinformation by design: Leveraging solutions to combat misinformation in the Philippines' 2025 election. *Data & Policy*. https://www.cambridge.org/core/journals/data-and-policy/article/disinformation-by-design-leveraging-solutions-to-combat-misinformation-in-the-philippines-2025-election/E7C163BB54FE808A0494539FC67974DD

Global Human Rights Defence. (2026, January 19). *Towards a trusting society: Exploring AI-powered deepfake threats to elections in the Philippines*. https://www.ghrd.org/towards-a-trusting-society-exploring-ai-powered-deepfake-threats-to-elections-in-the-philippines/

Global South Forum. (2025). *Deepfake: Disinformation by design*. https://www.globalsouthforum.org/article/deepfake-disinformation-by-design

Juju, Dominikus and MataMaya Studio. (2008). Teknik Menangkal Kejahatan Internet untuk Pemula [Techniques for Countering Internet Crime for Beginners]. Jakarta: Elex Media Komputindo.

OECD.AI. (2025, June 16). *Philippine officials spread AI-generated deepfake video, eroding public trust* [Incident report]. https://oecd.ai/en/incidents/2025-06-16-c1dc

PCIJ (Philippine Center for Investigative Journalism). (2025, December 31). *Rewriting reality: The information war that defined 2025*. https://pcij.org/2025/12/31/rewriting-reality-the-information-war-that-defined-2025/

Philippine News Agency. (2025). *AI deep fakes — technology and politics 2025* [Opinion]. https://www.pna.gov.ph/opinion/pieces/906-ai-deep-fakes---technology-and-politics-2025

Respicio & Co. (2026, February 10). *Identity theft using stolen IDs: How to report and protect yourself in the Philippines*. https://www.respicio.ph/commentaries/identity-theft-using-stolen-ids-how-to-report-and-protect-yourself-in-the-philippines

Reuters Institute for the Study of Journalism. (2025). *Philippines: Digital News Report 2025*. University of Oxford. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025/philippines

Reuters/Context. (2025, April 16). *Fake news and dirty politics flood Philippine social media*. Context by Thomson Reuters Foundation. https://www.context.news/big-tech/fake-news-and-dirty-politics-flood-philippine-social-media

Stowell, Louie. (2020). Panduan Berinternet Sehat dan Aman untuk Remaja [A Guide to Safe and Healthy Internet Use for Teenagers]. E-book. Esensi.

Syaripudin, Acep, et al. Internet Sehat: Pedoman Berinternet Aman, Nyaman, dan Bertanggung Jawab [Safe Internet: A Guide to Responsible, Comfortable, and Safe Internet Use]. E-book. ICT Watch.

The Diplomat. (2025, June 24). *Philippine senator's deepfake post raises fresh disinformation concerns*. https://thediplomat.com/2025/06/philippine-senators-deepfake-post-raises-fresh-disinformation-concerns/

Tsek.ph. (2025). *Filipino concern over online disinformation hits record high — Digital News Report 2025*. https://www.tsek.ph/filipino-concern-over-online-disinfo-hits-record-high-digital-news-report-2025/

UNICEF. Cyberbullying: Apa Itu dan Bagaimana Menghentikannya [Cyberbullying: What It Is and How to Stop It]. Accessed 20 September 2020 via https://www.unicef.org/indonesia/id/child-protection/apa-itu-cyberbullying

VERA Files. (2025). *Filipino concern over online disinformation hits record high — Digital News Report 2025*. https://verafiles.org/articles/filipino-concern-over-online-disinformation-hits-record-high-digital-news-report-2025

Yayasan Kita dan Buah Hati, ICT Watch, Kakatu. (2016). 17 Rumus Keren Internet Baik: Buku Panduan untuk Berinternet yang Bertanggung Jawab, Aman, Inspiratif dan Kreatif [17 Cool Rules for a Better Internet]. E-book.