DIGITAL SECURITY GUIDE FOR CONTENT CREATORS

DIGITAL SECURITY GUIDE FOR CONTENT CREATORS

Writers:
Sasmito
Adib Muttaqin Asfar

Reviewer:
Arif Kurniawan

Content Designer:
Eko Punto Pambudi

Cover Illustrator:
Imam Yunni

Translator:
Desy Nurhayati

November 2025

Alliance of Independent Journalists (AJI) Indonesia
Jalan Kembang Raya No. 6, Kwitang, Senen
Central Jakarta 10420
Phone 021-3151214, Fax 3151261
Email: sekretariat@ajindonesia.or.id
Web: www.aji.or.id

Supported by:

IMS
GOOD JOURNALISM | BETTER SOCIETIES

Funded by
the European Union

CONTENTS

Contents		3
Foreword		5
I. Introduction		**7**
II. Types Of Digital Attacks		**8**
A.	Spreading Rumor/Defamation	8
B.	Doxing	8
C.	Interception/Wiretapping	9
D.	Identity Impersonation	9
E.	Impersonation Of Victims' Accounts	9
F.	Hacking Or Taking Over Of Social Media Account	10
G.	Social Engineering	10
H.	Phishing	10
I.	Digital Device Seizure	10
J.	Gender-Based Digital Attacks	11
III. Digital Attack Mitigation		**12**
A.	Device Protection	12
1.	Physical Protection	12
a.	Avoid Buying Used Phones/Laptops.	12
b.	Never Leave Phone/Laptop Unattended.	13
c.	Use Protective Casing.	13
d.	Avoid Charging Through Public Usb Ports.	13
e.	Repair Only At Official Service Centers.	13
2.	Digital Protection	14
	On Phone	14
	On Laptop	17
B.	Online Data Protection	20
1.	Check For Your Data Spread Online	21
2.	Check For Data Breaches	22
3.	Delete Or Limit Access To Your Data	22
C.	Account Security	23
1.	Creating Stronger Passwords	24
2.	Two-Factor Authentication (2FA)	25
3.	Managing Account Privacy	26
4.	Account Management	27

IV. Handling Mechanism		**29**
A.	Loss Of Access To Accounts	30
1.	Identify The Problem	30
2.	Whatsapp Hacking	31
3.	Gmail Account Hacking	32
4.	Yahoo Mail Hacking	33
5.	Facebook Account Takeover	33
6.	Instagram Account Takeover	34
7.	Tiktok Account Takeover	35
8.	Youtube Account Hacking	36
B.	Buzzer Attacks	39
a.	Doxing	39
b.	Impersonating	39
c.	Online Gender-Based Violence/OGBV	40
C.	Being Target For Arrest	40
V. Emergency Contacts		**42**
A.	Technical Assistance Contacts	42
1.	Alliance Of Independent Journalists (AJI)	42
2.	Fast Response Team (TRACE)	42
3.	SAFEnet	42
4.	Access Now	42
B.	Legal Aid Contacts	43
	Greater Jakarta Area	43
	West Java and Banten Area	43
	Central Java and Yogyakarta Area	43
	East Java Area	44
	Bali and Nusa Tenggara Area	44
	Aceh and North Sumatera Area	44
	West Sumatera and Riau Area	45
	South Sumatera and Lampung Area	45
	Kalimantan Area	45
	Sulawesi and Papua Area	46
C.	Psychosocial Assistance Contacts	46
1.	Pulih Foundation	46
2.	LBH Apik Network in Various Cities	46

FOREWORD

In the ever-evolving digital era, content creators play a very important role in building narratives, delivering information, and influencing public opinion.

Although different from journalists who work under journalistic standards and codes of ethics, these content creators also provide diverse information on social media platforms in engaging ways, and sometimes their content is quite critical.

These content creators often share criticism, suggestions, and information with their social media followers. In fact, the number of their followers often exceeds that of the media itself. Their presence is now as important as that of media outlets that provide information.

This activeness, especially among those who have large audiences or discuss sensitive issues, increases the likelihood of becoming a target for hackers. Attacks such as doxxing, account hacking, and digital intimidation are often experienced by content creators who are considered to disrupt certain interests.

Unfortunately, not all content creators have a deep understanding of digital threats such as phishing, malware, or brute force attacks, which makes them more vulnerable to becoming victims of such attacks.

Data from research by PR2Media and the Alliance of Independent Journalists (AJI) in August 2024 revealed a shocking fact: 63.5 percent of 312 content creators in Indonesia have been victims of digital attacks in the past five years.

Some of the most common types of attacks include surveillance or stalking by unknown parties, phishing, which is fraud through emails and messages to steal personal data, bullying, threats, non-gender-based intimidation, and hacking or takeover of social media accounts.

The impact of these attacks cannot be underestimated. In addition to losing privacy, victims also face threats to their physical and emotional safety. Furthermore, losing access to digital accounts can be fatal, such as losing sources of income that depend on digital platforms.

Therefore, understanding digital threats and how to overcome them is not merely a choice but a necessity for content creators. Content creators need to understand and implement digital security measures to protect themselves and their work.

This “Digital Safety Guide for Content Creators” book comes as a response to the

urgent need of creators in facing various digital threats.

Beyond identifying threats, this guide also provides practical steps to secure devices, protect personal data, and manage risks in an increasingly dynamic digital environment. By understanding the right protection measures, content creators can ensure the sustainability of their work while maintaining audience trust.

This guide is written in a practical and easy-to-apply method. It explains how to ensure data encryption, create strong passwords, and what to do in case of an attack on social media.

By applying the security principles explained in this guide, it is expected that content creators can continue to create safely and free from digital threats.

The Alliance of Independent Journalists (AJI) Indonesia expresses its gratitude to Sasmito and Adib Muttaqin Asfar for writing this important book, as well as to the International Media Support (IMS) and the European Union for supporting the publication of this guide.

Happy reading, and always maintain your digital security!

Nany Afrida

President of The Alliance of Independent Journalists (AJI)

I. INTRODUCTION

A total of 63.5 percent of 312 content creators stated that they had experienced at least one type of digital attack over the past five years. This condition was revealed in the research "Digital Security of Content Creators in Indonesia" published by the Media Regulation and Regulator Watch (PR2Media) and the Alliance of Independent Journalists (AJI) in August 2024[1].

Four types of digital attacks deserve special attention because they are the most commonly experienced by content creators: being monitored/stalked, phishing, bullying, threats, non-gender-based intimidation, and hacking or takeover of social media accounts.

This research also shows that digital attacks against content creators threaten their physical and emotional security, privacy, and access to income sources. Therefore, content creators need to understand the types of content, digital attack prevention, and digital attack response.

1 https://aji.or.id/data/research-report-digital-safety-content-creators-indonesia

II. TYPES OF DIGITAL ATTACKS

The following are the types of digital attacks identified by PR2Media and AJI in the 2024 research "Digital Security of Content Creators in Indonesia":

A. SPREADING RUMOR/DEFAMATION

Digital rumor/defamation spreading refers to the distribution of false, baseless, or misleading information through digital media such as social media, websites, instant messaging applications, and other online communication platforms. This information is usually created or shared with a specific intent, such as harming an individual, group, or institution, or even causing public unrest.

Characteristics of digital rumor/defamation spreading include:

- Not based on facts
- Contains emotional elements
- Anonymous or unclear sources
- Viral or rapidly spread
- Uses engaging formats

Digital rumors or defamation are often delivered in the form of text, images, or videos with compelling or provocative narratives to increase their appeal.

B. DOXING

Doxing is a digital attack carried out by an individual or group who deliberately collects and publishes another person's private information online without permission, usually with malicious intent or to harm the victim. The term *"doxing"* comes from the word "documents" (dox), referring to personal documents or data exposed to the public.

Perpetrators of doxing usually have various motives, such as:

- Revenge or intimidation: to make the victim feel unsafe.
- Damaging reputation: spreading embarrassing information to tarnish someone's image.
- Encouraging further attacks: releasing information so others can issue threats, intimidation, or violence.

- Activism or hacktivism[2] : sometimes used to leak information about parties considered "dangerous" socially or politically.

C. INTERCEPTION/WIRETAPPING

Interception or wiretapping is the act of stealing or eavesdropping on digital communications without permission, carried out through hacking methods such as *Man-in-the-Middle (MITM)*[3] attacks, packet sniffing, or malicious applications such as spyware and keylogger programs. Wiretapping is considered a digital attack because it violates privacy, exploits sensitive data, threatens national security, and is often used for criminal activities such as extortion or fraud.

D. IDENTITY IMPERSONATION

Digital identity impersonation is a malicious act committed by someone pretending to be another person online for specific purposes, such as stealing data, committing fraud, or damaging the victim's reputation. Perpetrators usually use the victim's personal information—such as name, photos, or account credentials- obtained through phishing, hacking, or leaked data exploitation.

E. IMPERSONATION OF VICTIMS' ACCOUNTS

The creation of fake digital accounts under the victim's name is an illegal act in which the perpetrator creates an online account using the victim's identity without permission. This is usually done for malicious purposes such as fraud, spreading false information, or damaging reputation. Perpetrators often use the victim's personal data, such as name, photos, or email, taken from social media or other sources.

F. HACKING OR TAKING OVER OF SOCIAL MEDIA ACCOUNT

Hacking or takeover of social media accounts is the act of illegally accessing

2 Hacktivism is a form of cyberattack carried out by hackers for political or social purposes. They use technical skills to access, damage, or disrupt websites, systems, or networks as a means of expressing protest, influencing public opinion, or opposing policies deemed unjust. Hacktivism can take the form of DDoS attacks (disrupting access to a website), defacing (altering the appearance of a website), or leaking sensitive information to expose misconduct. Its main goal is to drive social or political change through the power of technology.

3 A Man-in-the-Middle (MITM) attack is a type of cyberattack in which the attacker secretly intercepts communication between two parties to steal or manipulate their data. In this attack, the perpetrator can monitor, alter, or even redirect messages without the victims' knowledge.

and taking control of another person's social media account. This is usually done through methods such as phishing, brute force attacks[4], malware[5], or by exploiting leaked personal data. The purposes may include identity theft, fraud, spreading harmful content, or damaging the victim's reputation.

G. **SOCIAL ENGINEERING**

SSocial engineering is a psychological manipulation technique used by perpetrators to trick individuals into revealing sensitive information or taking specific actions, such as disclosing passwords, personal data, or granting system access. This method often exploits trust, fear, or urgency through tactics such as phishing, pretexting, baiting, or vishing (voice phishing). Social engineering is dangerous because it exploits human weaknesses rather than technical vulnerabilities, making it difficult to anticipate.

H. **PHISHING:**

Phishing is a cyberattack in which the perpetrator impersonates a trusted entity or individual to deceive victims into providing sensitive information such as passwords, credit card numbers, or personal data. This attack is typically carried out through emails, text messages, or fake websites that appear legitimate to lure victims into the trap.

I. **DIGITAL DEVICE SEIZURE**

Digital device seizure refers to the act of forcibly taking or stealing digital devices such as mobile phones, laptops, or other gadgets with the intent of accessing sensitive data, sabotaging, or exploiting the information contained within. This threat not only involves the physical loss of the device but also digital security risks if the device is not protected with passwords, encryption, or tracking features.

4 Brute Force Attack is a hacking method in which the attacker tries every possible combination of passwords or encryption keys until the correct one is found. This process is performed automatically using software capable of testing combinations at high speed. Although simple, brute force attacks can be highly effective if the password used is weak or easy to guess.

5 Malware is a type of computer program designed to damage or disrupt computers, phones, or other electronic devices. Malware can infiltrate a device without the user's knowledge, and once inside, it can steal personal information, corrupt files, or slow down system performance. There are various types of malware, such as viruses, trojans, and ransomware, which can spread through emails, websites, or unsafe applications.

J. GENDER-BASED DIGITAL ATTACKS

SGender-based digital attacks are types of cyberattacks targeting individuals based on their gender identity, aiming to humiliate, intimidate, or control the victim. These attacks may include sexual harassment, verbal intimidation, online bullying, the distribution of private images or videos, and doxing (exposing personal information). Victims, especially women and gender minorities, are often targeted due to gender inequality and social stereotypes. Such attacks can cause severe psychological impacts and threaten the victim's privacy and personal safety.

From the above attacks, at least four types are most frequently experienced by content creators: being monitored/stalked, phishing, bullying, threats, and non-gender-based intimidation, and hacking or takeover of social media accounts.

The most common factors triggering digital attacks include the type of content uploaded, followed by certain relationships with other parties (such as public figures or individuals reported in the media), and personal beliefs.

III. DIGITAL ATTACK MITIGATION

Content creators need to have mitigation measures to prevent the nine types of digital attacks mentioned above, especially the four most common ones. Several steps that can be taken include protecting personal data in the digital space and securing digital assets.

However, this digital security guide for content creators begins with device protection, online data protection, and digital attack response. The guide prioritizes systematic protection of personal data to prevent content creators from falling victim to common digital attacks.

A. DEVICE PROTECTION

The threat of the above attacks always exists as long as devices, whether mobile phones or laptops, are connected to a network. Our behavior determines the level of risk or vulnerability to such attacks.

Things that should be done to protect digital devices include:

1. Physical Protection

a. *Avoid buying used phones/laptops.*

PUsed phones carry the risk of containing viruses or malware that you may not be aware of. It is best to avoid buying used devices. If you must purchase a used phone or laptop, make sure to carefully check the device's condition and history. Verify whether the device is registered as stolen or has security issues, for example, by checking the IMEI[6] or serial number to ensure authenticity. Ensure the device has been fully restored to factory settings and that no old data remains. Use security tools such as antivirus software and encryption to protect personal data. If possible, buy from trusted sellers offering warranties or return policies, and avoid transactions with unverifiable individuals.

6 IMEI (International Mobile Equipment Identity) is a unique number assigned to every mobile phone or device. This number acts as a "phone identity number" that distinguishes one device from another. With an IMEI, we can track or block a phone if it is lost or stolen, since this number cannot be changed. Therefore, if our phone goes missing, the IMEI can help locate or disable it to prevent misuse.

b. ***Never leave phone/laptop unattended.***

Leaving devices carelessly increases the risk of theft or unauthorized access, especially if they fall into the wrong hands. In addition, placing devices carelessly can cause physical damage due to impact or spilled liquids, which may harm internal components. To maintain privacy, protect personal information, and ensure the device functions properly, always store it in a safe and controlled place.

c. ***Use protective casing.***

A casing protects your phone from physical damage that could lead to data loss or loss of access to digital accounts.

d. ***Avoid charging through public USB ports.***

Avoid using USB ports in public places to charge your device, as they may contain malware (commonly referred to as juice jacking or data hijacking via USB)[7]. Charging ports in public places such as stations, airports, or shopping centers are often not secure. It is safer to use your personal charger or a power bank to minimize this risk.

e. ***Repair only at official service centers.***

Whenever possible, repair damaged phones or laptops at official service centers. You never know what might happen to your device during the repair process. If no official service center is available, look for a reputable and trusted non-official repair service with good reviews, but be aware of potential warranty risks. You can also contact the official service provider online, as some manufacturers offer remote repair guidance.

7 Committee to Protect Journalists, "Digital Safety Kit", July 30, 2019, https://cpj.org/2019/07/digital-safety-kit-journalists/#device

2. Digital Protection

On Phone

a. *Protect your phone with a lock (password, pattern, or fingerprint) to prevent unauthorized access.*

Do not leave your phone screen unlocked. Locks can take the form of a PIN or pattern (a combination of numbers), a password (a mix of numbers, letters, and other characters), or a fingerprint. Avoid using easily identifiable information such as birthdates, home or office numbers, or anything that can be guessed easily, to create PIN or passwords.

b. *Always update your operating system (OS), especially when prompted on your phone.*

Every version of Android, IOS, or other operating systems contains security vulnerabilities (bugs), and updates are designed to patch those weaknesses.

c. *Update applications when available.*

Always update your apps when updates are available, as these often include bug fixes, performance improvements, and, most importantly, security enhancements. Updating apps helps close security loopholes that hackers may exploit to access your personal data or device.

d. *Add extra locks to each application using a PIN, password, or fingerprint.*

Many smartphones offer encryption features to lock individual applications. Some apps also provide built-in lock options, such as WhatsApp or Signal.

e. *Change your phone's name so it is not easily recognized when connected to a network via Bluetooth or Wi-Fi.*

A publicly visible device name can reveal information about the phone's model, brand, or even the user's identity. This may make your device an easier target for hackers using brute force or other attack methods.

f. *Disable Wi-Fi and Bluetooth connections when not in use.*

All internet-connected devices have an address, also known as an Internet Protocol (IP) address. Keeping Wi-Fi or Bluetooth on unnecessarily can expose your device to detection by others. An exposed IP address may allow malicious software (malware) to access your device.

g. *Turn off location services when not needed.*

Disabling location services when unnecessary is essential to protect your privacy and prevent data misuse. Doing so reduces the risk of third-party tracking by advertisers, untrusted apps, or potential cyber threats.

h. *Avoid using public Wi-Fi in cafés, airports, and other public places.*

Public Wi-Fi can serve as an entry point for malware, data theft, and phone hacking.

i. *Use a VPN when accessing public Wi-Fi.*

Public Wi-Fi, such as in cafés, airports, or hotels, often lacks strong encryption, making it vulnerable to Man-in-the-Middle attacks and data theft. Without a VPN, personal data such as passwords, credit card information, or browsing history can be easily intercepted by malicious third parties. A VPN encrypts your internet connection, keeping your data secure even on unprotected public networks.

Do not use random or unverified VPN services, as they may compromise your security by collecting personal data, requesting access to sensitive information, or scanning installed applications. If you cannot afford a paid VPN, use a reputable free version such as Proton VPN, which offers strong privacy protections under Swiss data protection laws. Although free users have limited server options, the service provides unlimited access time and data.

j. *Install antivirus software on your phone.*

Installing antivirus software is crucial to protect your device from cyber threats such as malware, spyware, viruses, and malicious apps. Most smartphones—especially non-flagship models—

are vulnerable to attacks that can steal personal data, damage devices, or take control of them for illegal purposes. Antivirus software helps secure sensitive information such as passwords, credit card numbers, and private messages, and can block malicious websites, automatically update security systems, and scan and clean potential threats.

k. *Do not store sensitive files/documents on your phone*

   as this poses a risk if the device is lost, hacked, or infected with malware.

l. *Enable phone encryption.*
   - *Encryption is the process of converting data into secret code, making it unreadable to unauthorized users. If your phone is encrypted, its data cannot be accessed by anyone without permission.*
   - *This feature allows you to choose which applications to encrypt—for example, locking apps automatically after closing them or hiding credential-related apps (such as mobile banking, cloud drives, or data storage apps).*
     a. *On Android*

        The feature name varies by device; some call it File-Based Encryption. To find it, open Settings → Privacy & Security.

     b. *On IOS*

        Unlike Android, nearly all iPhones have Full Device Encryption (FDE) enabled by default from the factory settings.

m. *Limit app access permissions (location, camera, microphone, etc.)*

   A good app does not require access to all phone features. Apps should function properly even if they don't have full access.

   Restrict app permissions so they can only access what is necessary. For example, messaging apps do not need location access. If your chat app has location access, remove it unless required.

a. *On Android*

Go to Settings → Privacy → Permission Manager. You will find a list of your phone's features and which apps have access to them. Review each feature—such as the microphone—and see which apps can access it. You can modify or revoke access as needed. For instance, allow WhatsApp to access the microphone only while in use, not allowed all the time.

b. *On IOS*

Go to Settings → Privacy & Security, then review the list of apps with permission to access your device's features.[8] Control which apps are allowed to access features like the camera, photo library, or location.

On Laptop

a. *Lock the laptop with a password, code, or PIN.*

Set a strong password or PIN that is difficult to breach. Create a password using a combination of phrases, uppercase and lowercase letters, numbers, and other characters. Currently, it is recommended that the minimum password length be eight characters.

b. *Always update the operating system and applications.*

Just like other digital devices, there will always be security vulnerabilities (bugs) in every version of the laptop's operating system. System updates function to patch those vulnerabilities. For example, the number of security vulnerabilities found in the Windows operating system each year may vary, depending on the complexity and size of the system[9].

c. *Use a legal operating system.*

Operating system updates can only be performed if the system

8 David Nield, "How to manage app permissions on your iPhone," March 2, 2024, https://www.theverge.com/24087604/iphone-app-permissions-how-to

9 Microsoft's Windows operating system routinely releases monthly security updates that include fixes for various vulnerabilities. For example, in 2023, a total of 2,860 security flaws were discovered with varying levels of risk. However, not all vulnerabilities are found or publicly disclosed by Microsoft, as some may be unknown or not yet exploited.

is original or legal (not pirated). Illegal operating systems cannot be updated, leaving all vulnerabilities (bugs) unpatched.[10] If the legal version is too expensive, an open-source operating system based on Linux can be an alternative.

d. *Install antivirus or antimalware on the computer*

Each operating system includes built-in antivirus or antimalware software, such as Windows Defender on Windows laptops and XProtect or Malware Removal Tool (MRT) on MacBooks. Installing other reputable antivirus or antimalware programs is worth considering as a backup if the built-in software fails to detect a virus or malware.

e. *Regularly back up data/files stored on the laptop.*

Backing up data or files is crucial to minimizing the risk of loss, theft, or damage. Keep backup copies on another secure hard drive, such as an external hard disk. If possible, use the 3-2-1 backup method:

- The 3-2-1 Backup is a data backup strategy aimed at reducing the risk of data loss. The principle is to have three copies of data:
- The first copy is the original data stored on the main device (such as a phone, laptop, or computer).
- The second copy is a backup stored on a separate storage device, such as an external hard drive or local server.

The third copy is another backup stored in a different location, such as a cloud storage service or remote server.

This way, if the main device or local storage is damaged, the data remains safe and can be recovered from the other backup copies. This principle ensures that data stays protected even if one copy is lost or corrupted.

10 WannaCry is a ransomware from 2017. This malicious application spread through vulnerabilities in the Windows operating system, especially versions that were not updated or used pirated copies. This ransomware encrypts user data and demands ransom to restore access, threatening the loss of valuable data. Indonesia became the second most affected country by WannaCry because it used pirated OS.

f. *Cover the built-in laptop camera or webcam when not in use.*

This step reduces the risk of malware accessing your laptop's built-in camera. Some applications, including web-based ones, may request access to your camera or microphone. Always check the permissions of each application before granting access.

g. *Enable encryption on the laptop*[11].

By encrypting your laptop, the data stored on it cannot be read by unauthorized parties. For example, if the laptop falls into someone else's hands, they will not be able to easily read the data or documents inside.

- On Windows, enable BitLocker to encrypt the entire hard drive. For a detailed guide, visit https://t.ly/enkripsiwindows
- On Mac, enable FileVault. Go to the Apple icon > System Preferences > Security & Privacy > FileVault > turn ON.
- You can also use free software like VeraCrypt to encrypt hard drives and external storage.
- Encryption requires a strong and unique password to prevent unauthorized access.

h. *Enable the firewall on the laptop.*

A firewall is a network security system that monitors incoming and outgoing data traffic, allowing or blocking unsafe traffic. For example, it can block certain content or emails considered dangerous.

- On Windows, go to Settings > Update and Security > Firewall and Protection to enable the firewall.
- On Mac, click the Apple icon > System Preferences > Security & Privacy > enable Firewall.

i. *Turn off the location feature on the laptop.*

When the location feature is "on," your detailed location becomes easily traceable while connected to the internet, such as by web application operators.

11 Harlo Holmes, "Digital Security Fundamentals", 2023, freedom.press

- On Windows, go to Settings > Privacy > Location (turn off "Pin to Start") to disable the location feature.
- On macOS, go to System Preferences > Security & Privacy > disable Location.

j. *Rename the device.*

Every laptop has its own default name. Go to Settings and change the name to something unique. This helps prevent others from easily identifying your laptop when it is connected to a public network.

B. ONLINE DATA PROTECTION

On Tuesday, June 25, 2024, an X account under the name greschinov, which actively posts about the Gaza conflict, made a post that included a news article titled *"Indonesia's Imports from Israel Surge, Soaring by 1,204%."* The user also shared the full name of the journalist and the media outlet that published the article (Bisnis.com).[12]

The account greschinov then expressed several doubts about the article, published on Thursday, June 20, 2024, providing comparative data and ultimately accusing the report of being a hoax. The article written by the Bisnis.com journalist was based on data from Indonesia's Central Statistics Agency (BPS) regarding imports from Israel during April–May 2024. However, greschinov argued that the official data on the BPS website only covered up to April 2024.

"Where did they get the May 2024 data from? The claim is outrageous—up to 1,200%! What's going on here?" wrote greschinov.[12] "What's funny is that this news was immediately hyped by the flat-nosed Zionists, as if it were something to celebrate," he added.

In addition to calling the article a hoax, the greschinov account also shared the journalist's LinkedIn profile, saying, "This is the LinkedIn account of the article's author. You need to come forward and clarify—where did you get your data? If this is proven to be manipulation, this person should be fired or resign for intentionally fabricating data in the name of BPS!"

12 Alliance of Independent Journalists, "Indonesian Business Journalists Become Victims of Doxing," 2024, https://advokasi.aji.or.id/id/read/data-kekerasan/18889.html

Like journalists, critical content creators are vulnerable to attacks that exploit personal data scattered across various digital platforms.

Personal data can be weaponized for intimidation. Reexamine how much of your profile and personal information is publicly available on the internet, and consider whether that data should remain visible, or whether it's safer to remove it.

1. **Check for Your Data Spread Online**
    a. Open commonly used searchengines (Google, DuckDuckGo, or Bing).
    b. Type your name into the search engine and review the results.
    c. Search for other personal data such as your address, phone number, date of birth, or national ID number (NIK).
    d. Use private window or incognito mode to get broader search results.
    e. Use advanced search options or Boolean search techniques for more accurate results.
    f. In addition to text-based data (name, phone number, date of birth, address, NIK), also search for your photos using reverse image search (for example, on Google desktop or Google Lens on Android) to see where your images appear online.
    g. Search for your name on archival sites such as the Wayback Machine.
    h. Check for similar data belonging to your family members to ensure their information isn't being shared without consent.
    i. If you find unnecessary data, delete or restrict access to it (if you have control over it).
    j. If you don't have access to delete it, contact the website admin or account owner who posted the data and request removal.
    k. If you find sensitive data about yourself on the Wayback Machine, you can request its removal by sending an email to info@archive.org with the subject line: "Request for Exclusion from web.archive.org." In the email body, include the URL(s) of the information you want removed,

the time period, and any relevant details.[13] Note: Requests will be reviewed by the Wayback Machine team, but data removal is not guaranteed.

2. **Check for Data Breaches**
    - Check if your email account has been part of a data breach.
    - Use sites like www.haveibeenpwned.com, monitor.firefox.com, or periksadata.com.
    - Enter your email address, and the site will show whether it has appeared in known breaches.
    - If your email is found in a breach, immediately change the password for the affected service.

3. **Delete or Limit Access to Your Data**
    a. Ensure that the information you share on social media does not include sensitive data such as your home address, NIK, phone number, WhatsApp contact, or bank account number.
    b. Restrict access to your personal information on social media—especially for private accounts not used for campaigns or public content.
    c. Regularly review your privacy settings on social media platforms to make sure your public data does not put you at risk.
    d. Remind family, friends, or close contacts not to share sensitive data about themselves on social media or other digital platforms. This helps prevent them from becoming targets of attacks.
    e. To further protect your privacy, you can request Google blur your house on Street View:
        - Go to Street View and locate your home image.
        - Click the three dots on the top right corner, then select “Report a problem.”

13 Wayback Machine, “How do I request to remove something from archive.org?”, archive.org

14 https://antikorupsi.org/id/jokowi-masuk-nominasi-pemimpin-terkorup-icw-kena-doxing-dan-kami-tidak-takut

- Drag the red box over the area you want blurred.
- Choose “Request blurring” (options: A face, My home, My vehicle/a license plate, or A different object).
- Fill out the following fields and click “Submit.” (GAMBAR JALAN)

C. ACCOUNT SECURITY

Research findings by PR2Media and the Alliance of Independent Journalists (AJI) on Digital Security of Content Creators in Indonesia show that content creators face digital attack risks comparable to those faced by journalists, especially those who raise public interest issues. In fact, the risk for content creators is even greater, as they do not receive legal protection under the Press Law as journalists do.

For instance, one researcher from Indonesia Corruption Watch (ICW) became a victim of doxing conducted by the Instagram account @volt_anonym.[14] The doxing occurred on January 3, 2025, after the ICW researcher publicly expressed his views in several media outlets on January 1, 2025, regarding the nomination of Joko Widodo in the category of “Organized Crime and Corruption 2024” by the Organized Crime and Corruption Reporting Project (OCCRP).

The doxing involved the exposure of several personal data, including the researcher’s phone number, National Identity Card (KTP) number, residential address, phone device specifications, and even the last known location coordinates in the form of a Google Maps link. In the Instagram post, @volt_anonym included a caption with threatening language and strong insinuations endangering the researcher’s safety. ICW subsequently reported the case to

the Criminal Investigation Department (Bareskrim) of the Indonesian National Police.

The PR2Media and AJI research also revealed attacks experienced by the administrators of the Aksi Kamisan Bandung account. They reported that almost every social media post related to their activities was targeted by buzzer accounts. The attacks came in the form of negative comments, which appeared whenever the Aksi Kamisan Bandung Instagram account uploaded content discussing issues such as Papua or gender discrimination.

In addition, the administrators of Aksi Kamisan Bandung's account experienced multiple hacking attempts each time they posted content inviting people to join demonstrations. These attacks were not isolated; they were often accompanied by threats to identify or expose the administrators behind the Aksi Kamisan Bandung account.

The two examples above demonstrate that content creators are highly vulnerable to digital attacks. Therefore, content creators also need to take preventive measures to protect their digital accounts. Below are several fundamental steps content creators can take to secure their digital accounts.

1. **Creating Stronger Passwords**

   The most basic step to securing an account is using a strong password that is not easily breached.

   a. ***Use a passphrase, not a password.***

      - Review how secure your current password is. Visit www.howsecuremypassword.com or passwordmonster.com. Enter your password pattern (not the actual password) to check how easily it could be guessed.
      - To strengthen your password, combine uppercase letters, numbers, and other characters. For example: "K!l1m4nj4r0." Check again on the two sites above to see how long it would take to crack your password.
      - Next, use spaces and symbols to create a stronger passphrase, for example: "6unun6 K!l!m4nj4r0."
      - Enhance password security by mixing letters, numbers, symbols,

and both uppercase and lowercase characters.

- Create a password in the form of a memorable sentence, but avoid any personal information that is publicly known (such as birth date, home city, or child's name).

b. ***Use Password Manager***

- Never use the same password for multiple accounts. Mark Zuckerberg's account breach in 2016 occurred because he reused the same password across several social media accounts.
- Use a password manager application to store and manage different passwords for all your digital identities. This way, you only need to remember one strong master password for the password manager.
- Change your passwords regularly, at least once a year, to prevent risks if any password has been compromised.

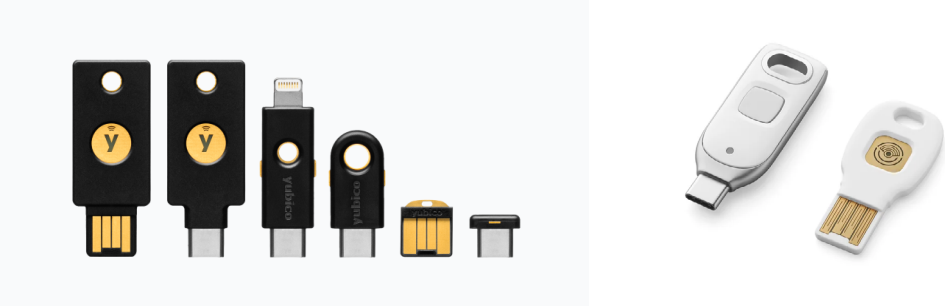
2. **Two-Factor Authentication (2FA)**

a. ***Two-step authentication (2FA)***

- Enable two-factor authentication (2FA) on every account that supports it. 2FA acts as a second gate after your main password. Even if your password is compromised, 2FA serves as an additional barrier against hackers.
- Each account has a different 2FA setup, but it generally uses a one-time password (OTP), usually in the form of numbers entered after your main password.
- 2FA can be implemented using apps such as Google Authenticator or similar applications.
- Avoid using SMS-based 2FA, as SMS messages can be intercepted and are not encrypted

b. ***Consider Using a Physical Security Key***

- One of the most secure forms of two-factor protection today is a physical key, such as YubiKey or Google Titan.



YubiKey (left) and Google Titan

- A physical key ensures that no one can access your account without having the key itself.
- The downside is that if you lose the physical key and do not have a backup 2FA method, you may permanently lose access to your account. Handle it carefully and ensure it does not get lost or fall into the wrong hands.

3. **Managing Account Privacy**

   a. Review the privacy settings on the digital platforms you use.

   b. Check what personal information is recorded by the platform.

      1) ***Google's privacy policy can be reviewed at https://policies.google.com/privacy.***

      2) ***Google's privacy settings can be checked at https://myaccount.google.com/intro/privacycheckup.***

      3) ***Information recorded by Facebook can be viewed at https://www.facebook.com/about/privacy.***

      4) ***Facebook's privacy settings can be adjusted through https://www.facebook.com/about/basics/manage-your-privacy.***

      5) ***Conduct similar reviews for other platforms you use, such as Twitter, Instagram, YouTube, and others.***

4. **Account Management**

   Sharing information or data through digital accounts has direct implications for the account owner's security. Review the information stored in each of your digital accounts and consider the potential consequences for yourself, your family, friends, colleagues, or sources if the account were to be leaked, hacked, or attacked.

   Here are key principles to consider in managing your digital accounts:

   1. Separate accounts based on purpose. For example, use different accounts for work (content distribution), activism (if you're involved in specific campaigns), and personal needs. Separating accounts helps reduce risks in case of a data breach or hacking, thus limiting exposure to only one account.
   2. Review your privacy settings and check what information is publicly visible, especially on social media accounts. Ensure that publicly visible information does not include sensitive data about you, your family, or close contacts that could be exploited for attacks.
   3. Delete publicly accessible sensitive information or data. However, before deleting anything, make sure to back up private data such as direct messages (DMs), emails, and other important files in a secure storage location—preferably on a lockable external hard drive.
   4. Audit all your accounts. Record every digital account you have created (email, social media, e-banking, and other digital platforms). List which accounts are linked together (e.g., Gmail linked to Facebook, X, and Instagram), which phone numbers they're associated with, what passwords they use, and what type of 2FA (two-factor authentication) is enabled.
   5. Delete unused accounts. After completing your account inventory, identify and permanently delete accounts you no longer use (not just log out). Before deletion, back up important data from those accounts and store it securely on an external hard drive.
   6. Review password strength. Check whether your passwords are strong enough. If any are weak, replace them with strong ones. Refer back to Section C.1 *Strengthening Passwords* for detailed guidance.

7. Enable two-factor authentication (2FA). Review which accounts haven't been protected by 2FA and enable the most secure authentication method available.
8. Monitor account activity. Open your account settings and check the "account activity" section. See which devices are logged into your account. If you find any unfamiliar devices, immediately remove their access.
9. Avoid accessing accounts from public or shared computers. If unavoidable, make sure to clear the browser's history and cache after logging out. This prevents others using the same computer from viewing your account activity.

IV. HANDLING MECHANISM

There are several steps content creators should take when they become the target of a digital attack or realize they are under threat.

1. **DON'T PANIC; CALM YOUR MIND BEFORE RESPONDING TO THE ATTACK.**

   Panicking can worsen the situation and lead to hasty decisions, such as disclosing sensitive information, clicking on malicious links, or taking actions that increase potential damage. By remaining calm, you can more objectively assess the threat and take planned steps to address it, such as disconnecting from the internet, changing passwords, or reporting the incident to authorities or cybersecurity professionals. Keeping emotions in check allows you to act more effectively to prevent or mitigate the impact of the digital attack.

2. **TAKE EMERGENCY STEPS TO IDENTIFY THE PROBLEM**

   Emergency steps to identify a digital attack include:

   1. **Disconnect from the internet:** Immediately unplug or disable your internet connection to prevent the attack from spreading or causing further damage.
   2. **Check for suspicious activity:** Review unusual device or account activity, such as unrecognized logins, changes in settings, or files that suddenly disappear or appear.
   3. **Run a security scan (antivirus):** Use updated antivirus or security scanning software to detect malware or viruses on your device.
   4. **Change passwords:** Update the passwords for all accounts linked to the compromised device, and ensure that two-factor authentication (2FA) is enabled.
   5. **Check login and activity logs:** For online accounts or applications, if still accessible, review login histories and activity logs to detect any unauthorized access.
   6. **Back up important data:** Immediately back up any data that remains safe to prevent larger information loss.
   7. **Contact service providers or cybersecurity professionals:** If necessary, reach out to those with cybersecurity expertise or civil society organizations

capable of handling cyberattacks (for example, the **Rapid Response Team (TRACE)**) for further assistance and recovery.

8. **Report the attack:** Report the incident to the service provider or online platform for account recovery, and to law enforcement if needed.

3. **DOCUMENT THE INCIDENT**

Immediately document any relevant evidence, including emails, direct messages, notifications, or other unusual signs of attack. The simplest way to do this is by taking screenshots and securely storing them as evidence.

4. **RECONSTRUCT THE TIMELINE OF THE ATTACK**

In a state of panic, this step can be quite difficult. Take a moment to calm yourself and ask key questions: when did the first signs of unusual digital activity appear, when did you lose access, and what actions did you take to respond? Grab a notebook or device and write down everything you remember in chronological order.

Here are the initial emergency steps you can take to respond to the attack:

A. **Loss of Access to Accounts**

Email, social media, and messaging platforms are vital tools for everyone, especially for content creators who address sensitive issues. Because of this, their accounts are more likely to become targets of digital attacks. One of the most common consequences is losing access to an account. If this happens, take the following steps:

1. ***Identify the problem***

a. Make sure your username and password are correct, double-check for typos or incorrect capitalization (Caps Lock).

b. Recall when you last changed your password, and try using your most recent one.

c. Check the most recent admin activity (if multiple admins manage the account) to ensure no one deleted the account. If the account was deleted (by an admin or others), it cannot be recovered.

d. Check whether you still have access to the recovery email or phone number linked to the account.

e. Review your email inbox for any login alerts or notifications indicating attempts to access your account from unfamiliar devices.

f. If the compromised account is on social media, view your profile (through another account or search engine) to check for unusual posts or profile changes.

g. If you notice deleted or unfamiliar posts, strange login notifications, or unauthorized changes to your recovery email or phone number, it means your account has likely been taken over.

h. If your username and password are correct but you still cannot log in, your account may have been blocked or suspended by the platform, possibly due to mass reporting or violations of community guidelines.

2. ***Whatsapp Hacking***

a. First, confirm whether your WhatsApp account has truly been hacked. If you are suddenly logged out of the app, it may indicate someone is trying to access your account from another device.

b. If the logout occurred but no messages were sent from your number, the attacker likely hasn't gained full control yet, since they would still need to enter PIN, especially if you've enabled Two-Step Verification (2FA) on WhatsApp.

c. If the attacker has started sending messages using your number, they've already taken control of your account and may have even enabled their own 2FA, making recovery more difficult.

d. Follow these steps to recover your account:

- Uninstall WhatsApp from your phone, then reinstall it.
- Register your phone number again and wait for the 6-digit verification code sent via SMS. Enter the code immediately once received.

- If you don't receive the SMS, wait for up to 10 minutes, then select the "Call me" option to get your verification code via an automated phone call.
- When you receive the call, note the 6-digit code and enter it into WhatsApp to verify your account.
- Once access is restored, immediately enable Two-Step Verification (PIN + email) to protect against future hijacking.
- If WhatsApp asks for a two-step verification PIN that you didn't set, it means the hacker activated it. You'll need to wait 7 days before you can log in without that PIN.
- Report the stolen account to WhatsApp by emailing support@whatsapp.com with the subject line: "Lost/Stolen: Please deactivate my account."

e. Seek help if recovery fails

- Stay calm and record the timeline of the hacking incident.
- Document all signs of breach—notifications, emails, and recovery steps—by taking screenshots.
- Contact an emergency support network for assistance (see the Contact Directory section at the end of this guide).

3. ***Gmail Account Hacking***

a. If you can still access your Gmail account, immediately change your password and enable two-step verification (2FA) if you haven't done so already.

b. If you cannot log in, go to the account recovery page via this link: https://s.id/PemulihanGmail. You'll be asked to enter your recovery account (email or phone number) and follow the on-screen instructions to regain access.

d. For a complete guide on Gmail account hacking and recovery, visit: https://support.google.com/accounts/answer/7682439?hl=id.

e. Seek help if recovery fails:

- Stay calm and record the chronology of the hacking incident

- Document all evidence—notifications, emails, and recovery steps—by taking screenshots.
- Contact emergency support channels for further assistance (see the Contact Directory section at the end of this guide).

4. ***Yahoo Mail Hacking***

   a. Reset your password by visiting https://help.yahoo.com/kb/SLN27051.html.

   b. Enter your Yahoo Mail address.

   c. Choose your preferred reset method, via registered phone number or recovery email. Using a recovery email is generally safer than using a phone number.

   d. You'll receive a verification code through email or SMS. Enter the code on the Yahoo recovery page.

   e. Create a strong new password using a mix of letters, numbers, and spaces.

   f. Seek help if recovery fails:

      - Stay calm and record the chronology of the hacking incident.
      - Document all evidence—notifications, emails, and recovery steps—by taking screenshots.
      - Contact emergency response services listed in the Contact Directory at the end of this guide.

5. ***Facebook Account Takeover***

   a. To check if someone else has accessed your Facebook account without permission, go to Settings → Security and Login Info, then reviewe the section "Where You're Logged In." This will show a list of devices (laptops or phones) currently accessing your account.

   a. *b. If you find a device that isn't yours, click the three dots on the right and select Log Out. Then immediately change your password to a stronger one.*

c. If your account has been hacked and the password has been changed, Facebook will send a notification email to your registered address. Check your inbox for this alert.

d. In that email, Facebook provides a "Click here" link if you didn't make the password change. Follow the link and answer the recovery questions provided to restore your account.

e. To report a hacked account, visit https://www.facebook.com/hacked.

f. Seek help if recovery fails:

- Stay calm and create a chronology of the hacking incident.
- Document all evidence—notifications, emails, and recovery steps—by taking screenshots.
- Contact emergency support channels listed in the Contact Directory at the end of this guide.

6. ***Instagram Account Takeover***

a. If you're using a laptop, you can check whether someone has accessed your Instagram account by going to Settings → Login Activity. This page shows the devices and locations where your account has been accessed.

b. If you find a device you don't recognize, click the arrow on the right and select Log Out.

c. If you can no longer log in, check your registered email for a notification from Instagram. The platform sends alerts whenever there's a login from a new device or a password change.

d. Click "Secure Your Account Here," which will take you to a page where you can reset your password. Enter a strong and unique password.

e. If the account remains difficult to recover, report the issue to Instagram:

- On the login screen, tap "Get help logging in" (on Android) or

"Forgot password?" (on iOS).

- Enter your username, email, or phone number, then tap Next.
- Tap "Need more help?" and follow the on-screen instructions.
- Make sure you use a secure email address that only you can access.
- Once you've submitted your request, wait for Instagram's response with further recovery steps.

f. Seek help if recovery fails:

- Stay calm and record the timeline of the hacking incident.
- Document all evidence—notifications, emails, and recovery steps—by taking screenshots.
- Contact emergency support channels listed in the Contact Directory at the end of this guide.

7. ***TikTok Account Takeover***

a. Signs your TikTok account may have been hacked:

- Your password or linked phone number has been changed.
- Your username or nickname has been altered.
- Videos you uploaded have been deleted or new videos appear without your consent.
- Your account is sending messages without your knowledge.

b. Although TikTok's official page doesn't specify a detailed recovery process for lost accounts, here are the steps you can take using available security features:

- Open the TikTok app on your phone and select "Forgot password?"
- You'll be asked to enter the contact information linked to your account (phone number or email, depending on your recovery setup).
- Tap "Reset" to receive a recovery code. The code will be sent

to your phone via SMS or to your email.

- Enter the recovery code in the password reset section. If successful, you can create a new, stronger password.
- If all goes well, the hacker won't know your new password. Strengthen your account security by enabling two-factor authentication (2FA) — ideally using a physical passkey if available.

c. Remove suspicious connected devices[15]

- Check whether anyone has logged into your TikTok account from another device.
- Go to Settings and Privacy → Security → Select Your Devices.
- Remove any suspicious or unknown devices.
- Account security and device management tools can also be accessed via the "My account has been hacked" page on TikTok's official website.

d. Report the hacking incident to TikTok.
You can report issues directly through TikTok's Report a Problem page at support.tiktok.com or https://support.tiktok.com/en/log-in-troubleshoot/troubleshooting/report-a-problem

e. Seek help if recovery fails:

- Stay calm and document the chronology of the hacking incident.
- Record all signs of hacking—notifications, email alerts, and recovery steps—using screenshots.
- Contact emergency support channels listed in the Contact Directory at the end of this guide.

8. ***Youtube Account Hacking***

Every YouTube account is linked to a Google account. However,

15 Tiktok, "My account has been hacked", https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked

there are cases where a compromised YouTube account cannot be restored even after the associated Gmail account has been recovered.

In 2022, the YouTube channel of a gender minority activist group was hacked. The attacker easily took over the account because the password was simple (easy to guess) and rarely changed. Recovery efforts began by regaining access to the Gmail account associated with the YouTube channel, but the channel itself could not be recovered. After several attempts, YouTube eventually deleted the channel, citing policy violations. The group repeatedly appealed through the link provided in the notification email, but YouTube stated that the account no longer existed. The channel was finally restored only after the case was reported to Google with assistance from an organization experienced in handling digital attacks.

a. *Recognizing Signs of Hacking*
   - Unexpected changes to your account — such as profile picture, description, email settings, AdSense, or outgoing messages you didn't send.
   - Videos appear on your channel that you didn't upload. This indicates someone else has uploaded content using your Google account. Check your email for notifications warning of unfamiliar uploads or logins from unknown devices.

b. *Account Recovery*[16]
   1. *Recovering your Google/Gmail account*
      - *If you can still log in, immediately change your password to a stronger one and enable 2FA (via an authenticator app or physical passkey).*
      - *If you can't log in, follow the Google Account Recovery steps described in Section 3 of this guide.*
      - *Repeat the same steps for other Google accounts you own.*
   2.. *Once your Google account is secured, your YouTube account should be accessible again.*

16 Google, "Recover a hacked YouTube channel", https://support.google.com/youtube/answer/76187?hl=en

3. *For detailed recovery steps, visit the Recover a hacked YouTube channel page*

c. *Seek help if recovery fails*

- Stay calm and reconstruct the timeline of the hacking incident.
- Document all signs of hacking (notifications, email alerts, and recovery steps), preferably with screenshots.
- Contact emergency support services listed in the Contact Directory at the end of this guide.

d. *Restore your YouTube channel to its pre-hack state[17].*

If hackers managed to take over your YouTube channel, they may have made changes to both the channel and the linked Google account.

a. Document all traces left by the hacker, including evidence from your linked email account. You can archive them using tools such as perma.cc or archive.is.

b. Remove all unauthorized users connected to your channel:

- If you use Channel Permissions, sign in to YouTube Studio → Settings → Permissions. Select the username you wish to remove and click "Remove access."
- If you use a Brand Account, open the Brand Accounts section in your Google Account settings and follow similar steps to remove access.

e. *Restore your channel settings. If the hacker changed your channel name, profile image, or banner, revert them to the original state to avoid permanent deletion.*

f. *Permanently delete all videos uploaded by the hacker.*

g. *For detailed guidance on restoring your channel, see Clean up a hacked YouTube channel.*

17 Google, "Clean up a hacked YouTube channel", https://support.google.com/youtube/answer/14849770#zippy=%2Cdelete-hacker-uploaded-videos-without-violations%2Crestore-your-channels-basic-info-and-branding%2Cremove-any-unknown-users-from-your-channel-or-account

B. **Buzzer Attacks**

There are various forms of attacks carried out by *buzzers*, including: trolling (creating chaos through comments, arguments, or false information to provoke negative reactions); doxing (revealing the personal identity of a targeted individual); impersonating (faking or mimicking another person's account); and Online Gender-Based Violence/OGBV (targeted digital abuse based on gender).

The following are several recommended response steps, adapted from Chapter 6 of the Digital Security Guide for Journalists (2022)[18].

a. ***Doxing***

- If a journalist's home address is disclosed, the media company should find a temporary safe house for the victim and their family until the attack subsides.
- Report posts containing doxing to the platform and block the perpetrator's account.
- If the perpetrator discloses the phone number and the victim receives many disturbances, the phone should be turned off temporarily, and consider changing the phone number later.
- If the perpetrator exposes the victim's bank account number, credit card, or other financial account information, immediately contact all related financial institutions and report the violation.
- Temporarily closing social media accounts is the best option if the attack escalates.
- Report the doxing to the police by bringing documentation and links as evidence.
- Archive through https://perma.cc/ or https://archive.is/.

b. ***Impersonating***

- Create an announcement about the fake account so that the public (audience and followers) are not deceived.

18 https://aji.or.id/system/files/2024-07/layoutpanduankeamanandigitaluntukjurnalisfixcompressed_4.pdf

- Report any account that uses the identity of your media outlet or journalists to the platform provider so that the fake account can be taken down.

  1. Reporting fake accounts on Facebook: https://s.id/akunpalsuFB
  2. Reporting fake accounts on Twitter or X: https://help.x.com/en/forms/authenticity/impersonation
  3. Reporting fake accounts on Instagram: https://s.id/akunpalsuIG
  4. Reporting fake Gmail accounts: https://s.id/akunpalsuGmail

c. ***Online Gender-Based Violence/OGBV***

- Report or block accounts, posts, or comments that contain harassment, including online gender-based violence (OGBV), to the platform.
- Seek support from civil society organizations that focus on freedom of expression issues (for example, the nearest chapter of the Alliance of Independent Journalists/AJI or SAFEnet).
- Seek assistance from institutions that provide services for victims of sexual harassment or violence (for example, LBH Apik or organizations that protect women's rights), and obtain legal and psychosocial support from these institutions.
- Report the violence and harassment experienced by the victim to the police, whether it occurs via phone, SMS, chat, or other social media, including documentation of the harassment or violence.

C. **Being Target for Arrest**

- If you are in a vulnerable situation or at risk of being targeted for arrest or detention (for example, due to your content), consider logging out of all related accounts and any accounts that store sensitive data or information.
- Clear your browser history. Ensure that all sensitive data or information

is securely stored on an encrypted (locked) hard drive.

- Contact a legal aid organization (LBH), the Witness and Victim Protection Agency (LPSK), or the nearest civil society organization that can provide assistance and protection, including a safe house.

V. EMERGENCY CONTACTS

A. TECHNICAL ASSISTANCE CONTACTS

In the event of an attack or when content creators require mitigation measures, the following institutions can be contacted for assistance:

1. **Alliance of Independent Journalists (AJI)**

   Complaint link: https://safetycorner.aji.or.id/node/6511

2. **Fast Response Team (TRACE)**

   Complaint link: https://lapor.trace.mu/

3. **SAFEnet**

   Complaint link: https://aduan.safenet.or.id/

4. **Access Now**

   Complaint link : https://www.accessnow.org/help/#contact-us

B. LEGAL AID CONTACTS

Greater Jakarta Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Pers	Jl. Kalibata Timur IV G No. 10 Kalibata, Pancoran, Jakarta Selatan	Telp. 021-79183485, 0821-4688-8873	secretariat@l bhpers.org
YLBHI	Jl. Diponegoro No. 74, Menteng, Jakarta Pusat 10320	Telp. 021-3929840 Faks. 021 31930140	info@ylbhi.or.id
LBH Jakarta	Jl. Pangeran Diponegoro No.74 , Menteng, Jakarta 10320	Telp. 021-3145518 Faks. 021-3912377	lbhjakarta@bantuanhukum. or.id
PBHI	Jl. Hayam Wuruk No.4, RT.9/ RW.5, Kb. Klp., Kec. Taman Sari, Jakarta 10120	Telp. 021-3859968	
LBH Apik Jakarta	Jl. Raya Tengah No. 31 RT 01 RW 09 Kampung Tengah Kramat Jati Jakarta Timur 13540	Telp. 021–87797289, 0813-888226699 Faks. 021–87793300	LBHAPIK@gmail.com

West Java and Banten Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Bandung	Jl Kalijati Indah Barat No 8, Antapani Bandung	Telp. 0821-2017-1321	konsultasi@l bhbandung. or.id
LBH Apik Jabar	Jalan Beringin No. 9 Kemiri Muka, Beji, Kota Depok, Jawa Barat	Telp. 0813-8030-4852	lbhapikjawab arat@gmail. com
LBH Apik Banten	Jln. Raya Pandeglang Km. 3, Komp. Tembong Indah, Sempu, Kota Serang – Banten	Telp. 0254-227969 Faks. 0254-227969	

Central Java and Yogyakarta Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Semarang	Jl. Jomblangsari 4 No. 17, Jomblang, Candisari, Kota Semarang	Telp. 024-86453054, 0882-2890-2001	office.lbhsem arang@ylbhi. or.id
LBH Apik Semarang	Jalan Poncowolo Timur Raya No. 455 Semarang, Jawa Tengah (masuk melalui jalan Indraprasta)	Telp. 024-3510499	apiksemaran g@yahoo.com

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Yogyakarta	Jl. Benowo No.309, Winong, RT 12/RW 03, Prenggan, Kec. Kotagede, Kota Yogyakarta, Daerah Istimewa Yogyakarta 55172	Telp. 0274-4351490	kalabahulbhjo gja@gmail.com
LBH Apik Yogyakarta	Jalan Nogodewo 12, Gowok, Sleman, Yogyakarta	Telp. 0274-379614, 08179410624	apik_jogja@y ahoo.com

East Java Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Surabaya	Jl. Kidal No.6, Pacar Keling, Kec. Tambaksari, Kota SBY, Jawa Timur60131	Telp. 031-5022273	bantuanhuku msby@ gmail.com
LBH Surabaya Pos Malang	Jl. Teluk Perigi Rt 01, Rw 10 Tirtomoyo, Kec. Pakis, Kab. Malang, Jawa Timur 65154	Telp. 081252226205	lbhmalang@ylbhi.or.id
LBH APIK-Kota Batu	Jalan Kapten Ibnu, Ruko 8 RT03/RW13, Kel Sisir, Batu, Kota Batu, Jawa Timur	Telp. 6281336554420	lbhapikkotaba tu@gmail.com

Bali and Nusa Tenggara Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Bali	Jalan Plawa No. 57, Denpasar Timur, Denpasar, Bali	Telp. 0361-223010	lbhbali@indo.net.id
LBH APIK Bali	Jalan Suli 119 – A3, Denpasar Timur	Telp. 0361–9272245, 081337325896	lbh.tentrem@ gmail.com
LBH APIK NTT	Jalan Sam Ratulangi II no.33B Walikota Baru, Kel. Oesapa Barat, Kec. Kelapa Lima, Kota Baru, Kupang 85228.	Telp. 0380 823647	lbhapik.ntt@g mail.com
LBH APIK NTB	Jalan Angklung Raya no. 2 Karang Bedil, Mataram, Lombok, NTB	Telp. 0817-5768-4 96, 0823-3959-3221	lbhapikntb17@gmail.com

Aceh and North Sumatera Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Banda Aceh	Jalan Sakti Lorong LBH Banda Aceh No.1, Desa Pango Raya, Ulee Kareng, Banda Aceh 23119	Telp. 0651-8057952	lbh_aceh1995@yahoo.com

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH APIK Aceh	Jalan Tengku Daud No. 147, Panggoi, Muara Dua, Kota Lhoksmeumawe, Aceh 24355	Telp. 0645-43150	lbhapikaceh @gmail.com
LBH Medan	Jalan Hindu No.12 Medan 20111, Sumatera Utara, Indonesia	Telp. 061-4515340 Faks. 061-4569749	lbh_medan@ yahoo.com, kantor@lbhm edan.org
LBH APIK Medan	Jalan Jermal V No. 1C, Denai, Medan Denai	Telp. 0821-5753-9308, 0282-115063359	admlbhapikm edan@ gmail.com

West Sumatera and Riau Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Padang	Jalan Pekanbaru No 11A, Kota Padang, Sumatra Barat	Telp. 0751-7056059	
LBH Pekanbaru	Jl. Sapta Taruna No.51, Tengkerang Utara, Kec. Bukit Raya, Kota Pekanbaru, Riau 28289	Telp. 0761-45832, 0811-765-832	info@lbhpeka nbaru.or.id

South Sumatera and Lampung Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Palembang	JL. HBR Motik No.12A Rt.29 Rw.9 Kel.Karya Baru Kec. Alang-alang Lebar Kota Palembang	Telp. 0711-5610122, 0813-6930-0442	lbhpalemban g@ylbhi. or.id
LBH APIK Sumatera Selatan	Jalan Sekip Bendung Dalam No. 009 RT. 035 RW. 009, Kel. 8 Ilir, Kec. Ilir Timur III, Kota Palembang	Telp. 0821-7770-0069	yayasanlbhap iksumsel@g mail.com
LBH Bandar Lampung	Jalan Sam Ratulangi, Gg Mawar 1, Nomor 7, Gedong Air, Bandar Lampung 351117	Telp. 0721-5600425	bantuanhuku mlampung@ gmail.com

Kalimantan Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Kalimantan Barat	Jl. Dr. Sutomo, Komplek Batara Indah 4 No. 16 D, Pontianak, Kalimantan Barat	Telp. +62 812-5880-6816	lbhkalbar@ylbhi.or.id
LBH APIK Pontianak	Jalan Alianyang No. 12A Pontianak, Kalimantan Barat 78116	Telp. 0561–766439	apik_ptk@ya hoo.com

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Samarinda	Jl Wijaya Kusuma II No 50, Air Putih, Samarinda Ulu Samarinda	Telp. 0821-5133-15537	lbhsamarinda @ylbhi. or.id, lbhsamarind@ gmail.com
LBH APIK Kalimantan Timur	Jalan Sultan Sulaiman, Perum Citra Gading Blok B2 No. 9 Samarinda – Kalimantan Timur	Telp. 0541-4106482, 0812-5822-7 15, 0812-5826-828	ylbhapikkalti m@gmail. co m
LBH Palangka Raya	Jl. Parawei, Perum Casadova blok B, No. 10, Kota Palangka Raya, Prov. Kalimantang Tengah	Telp. 0857-8696-8317	ylbhi.lbh.pala ngkaraya@g mail.com

Sulawesi and Papua Area

INSTITUTION	ADDRESS	PHONE	EMAIL
LBH Manado	Jl.A Manonutu No. 29, Wanea, Kota Manado 95116	Telp. 0431-8806473; 085256303949; 085240523068	ylbhi.lbhmana do@ gmail.com
LBH APIK Manado	Jalan Bethesda 6 No. 77, Ranotana ling II, Manado - 95116	Telp. 0431-824132	
LBH Makassar	Jl. Nikel 1 Blok A22 No.18 Kota Makassar, Kode Pos 90222	Telp. 0411-4677699	lbhmks.ylbhi@gmail. com
LBH APIK Makassar	Jalan Perintis Kemerdekaa n, Perum Budidaya Permai Blok D no. 3, Makassar, Sulawesi Selatan		lbhapiksulsel.or.id
LBH APIK Palu	Jalan Teluk Tomini No. 8B, Kota Palu - 94221	Telp. 0451-4015986, 0811-4540-1616	lbhapik_sulte ng2@ yahoo.com
LBH Papua	Jl. Gerilyawan No. 46 Jayapura, Papua 99532	Telp. 0967-581710; 08124808635	lbh.papua@y ahoo.co.id
LBH APIK Jayapura	Jalan Raya Sentani, Padang Bulan, Abepura, Jayapura, Papua 99351	Telp. 0411-590147, 0812-9400-7696	lbhapikjayapu ra17@ gmail.com

C. PSYCHOSOCIAL ASSISTANCE CONTACTS

1. Pulih Foundation

Address : Jl. Teluk Peleng 63 A Komplek AL-Rawa Bambu Pasar Minggu Jakarta 12520, Phone: 021-788 42 580, 021- 982 86 39

E-mail : pulihfoundation@gmail.com ; pulihcounseling@gmail.com

2. LBH Apik Network in Various Cities