ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

IMS
GOOD JOURNALISM | BETTER SOCIETIES

Funded by
the European Union

Guidelines to Develop Digital Security SOP for Media Companies

Guidelines to Develop Digital Security SOP for Media Companies

Writers:
Sasmito
Adib Muttaqin Asfar

Reviewer:
Arif Kurniawan

Layout and Cover Designer:
Krisna Sahwono

Translator:
Desy Nurhayati

November 2025

ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

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

Foreword

Not an Option, but a Necessity

In the increasingly complex digital era, digital security for media companies is no longer a choice but an urgent necessity. The media serves as the fourth pillar of democracy—revealing the truth and delivering accurate information to the public. Its increasingly strategic role has also made media companies a prime target for various digital threats, ranging from hacking and cyberattacks to communication interception. Consequently, critical and independent media face a threatening domino effect.

In recent years, attacks on media companies in Indonesia have risen sharply, coming from state actors, criminal groups, and individuals with specific interests.

Without a strong digital security system, media organizations face serious risks. One major risk is operational disruption, where ransomware or system breaches can paralyze newsroom activities and hinder news production.

Beyond direct attacks on media companies, disinformation and data manipulation have also become significant challenges. In an age increasingly dominated by hoaxes and digital propaganda, public trust in the media can collapse if there are security gaps that allow outsiders to alter or insert false information into news content.

Digital security is not just about protecting internal systems but also ensuring that the information delivered to the public remains trustworthy and free from manipulation by vested interests.

A study conducted by the Media Regulation and Regulator Watch (PR2Media) in collaboration with the Alliance of Independent Journalists (AJI) from May 29 to June 19, 2024, involving 116 media companies, revealed that the level of digital security among online media organizations remains low. This is reflected in a Digital Security Index score of only 19.71 out of a maximum of 31 points.

PR2Media used five indicators to assess digital security practices within media companies. The study found that only the indicator related to the presence of dedicated IT resources received a good score. Meanwhile, four other indicators—SOP implementation, education, security audits, and risk assessments—showed low or inadequate results, indicating the need for stronger digital security strategies in the media sector.

This study prompted AJI Indonesia to publish the Guidelines to Develop Digital Security SOP for Media Companies.

The guide aims to help media organizations implement comprehensive digital security measures, including data protection strategies, safety practices for journalists, communication encryption, cyberattack mitigation, and actionable steps to build a safer media ecosystem.

By understanding the existing challenges and applying the right protective measures, media companies can continue to carry out their mission more safely and effectively—without fear of increasingly sophisticated digital threats.

AJI Indonesia hopes that the Guidelines to Develop a Digital Security SOP for Media Companies will serve as a practical reference for chief editors, IT managers, journalists, and the broader media ecosystem in building a stronger digital security framework.

It must be emphasized that digital security is not the responsibility of a single individual or department within a media organization. It is a shared commitment to safeguarding press freedom and ensuring that the media remains a credible and reliable source of information.

AJI extends its gratitude to Sasmito and Adib Muttaqin Asfar for writing this highly important book. It is hoped that the Guidelines to Develop Digital Security SOP for Media Companies will serve as a starting point for media organizations that are still uncertain about where to begin.

This guide marks the first step toward a more resilient media ecosystem in the digital era.

Nany Afrida
President of The Alliance of Independent Journalists (AJI)

CHAPTER I
Introduction

A survey conducted by the Media Regulation and Regulator Watch (PR2Media) in collaboration with the Alliance of Independent Journalists (AJI) between May 29 and June 19, 2024, across 116 media companies, revealed that the level of digital security among online media organizations remains unsatisfactory.[1] The survey revealed that the Digital Security Index for online media companies reached only 19.71 out of a maximum score of 31. This score was derived from three main aspects: experience with digital attacks, digital security practices, and perceptions of digital security.

Among these three aspects, the digital security practices component recorded the lowest score, 5.03 out of a possible 11—indicating a significant gap. Meanwhile, the scores for experience with digital attacks were relatively good, and perceptions of digital security scored positively.

PR2Media used five indicators to evaluate the digital security practices of media companies: the existence of Standard Operating Procedures (SOPs) for digital security; security education and training for media workers; the

[1] https://aji.or.id/data/research-report-digital-security-media-companies-indonesia

presence of dedicated information technology resources to prevent digital attacks; the implementation of digital security audits within the company; and the implementation of digital security risk assessments for employees and contributors.

Of these five indicators, only the presence of dedicated IT resources was rated as satisfactory. The remaining four indicators were found to be inadequate or poor.

PR2Media also conducted an online focus group discussion on July 9, 2024, involving 13 selected participants from among the survey respondents. The discussion aimed to deepen the survey's findings on the state of digital security in media companies. It provided a more comprehensive picture of actual digital protection practices. For instance, although most respondents reported having a digital security SOP, the discussion revealed that these SOPs were generally limited to internal IT team guidelines, were not always documented in writing, and did not cover digital assets related to journalistic work—such as digital application accounts used by reporters. Similarly, regarding security education and training, the discussion found that such programs were not always organized by the media companies themselves. Many were instead conducted by external organizations, including AJI Indonesia, IREX, and SAFEnet.

Regarding the aspect of experience with digital attacks, which scored relatively well, the research found that 71.6 percent of the 116 respondents had experienced at least one of nine types of digital attacks identified in the survey. The three most common types of attacks were buzzer or troll attacks, website attacks, and false or baseless reports targeting media organizations' social media accounts.

Among the nine types of digital attacks, the most frequently experienced were "buzzer/troll attacks" (score 3.07) and "website attacks" (score 3.09), while the least common were "ransomware attacks" (score 3.88) and "interception/surveillance" (score 3.87).

According to data from the Alliance of Independent Journalists (AJI), there were 14 digital attacks recorded throughout 2023. The most frequent type was hacking (7 cases), followed by website or social media account suspensions (3 cases), website attacks (3 cases), and doxing (1 case).

Based on these findings, media companies must strengthen their digital security practices. As an initial step, a digital security Standard Operating Procedure (SOP) is needed to serve as a common reference for all employees within the media organization, not merely an internal guideline for the information technology team.

CHAPTER II
Types of Digital Attacks

The following are the types of digital attacks identified by PR2Media and AJI in their 2024 study titled "Digital Security of Media Companies in Indonesia":

a. Malware

The acronym malware, derived from malicious software, refers to any program or file designed to harm users of computers or mobile devices. Forms of malware may include viruses, worms, Trojan horses, and spyware. Such programs can perform a range of malicious activities, including data theft, encryption, or deletion; unauthorized alteration of core computing functions; and surreptitious monitoring of user activity without permission.

b. Doxing

Doxing refers to a digital attack carried out by an individual or group that intentionally gathers and publishes another person's private information online without authorization, often with the intent to harass, intimidate, or harm the target. The term "doxing" is derived from "documents" (dox), referring to personal files or data that are made publicly accessible.

The perpetrators of doxing may act with a range of motives, such as:

- Retaliation or intimidation: intended to make the victim feel unsafe.
- Reputation damage: spreading embarrassing information to smear a person’s name.
- Enabling further attacks: exposing information so others can carry out threats, intimidation, or violence.
- Activism or hacktivism[2]: sometimes used to leak information about individuals or groups deemed socially or politically “harmful.”

c. Interception

Interception, also known as digital wiretapping, involves the unauthorized access or monitoring of digital communications. Such activities are commonly executed through hacking techniques like Man-in-the-Middle (MITM)[3] attacks, packet sniffing, or the deployment of malicious applications, including spyware and keyloggers. This practice constitutes a digital attack as it infringes upon individual privacy, compromises sensitive information, poses risks to national security, and is frequently exploited for criminal purposes such as extortion and fraud.

d. Social Engineering

Social engineering refers to the use of psychological manipulation by threat actors to trick individuals into revealing confidential information or performing actions that compromise security, such as disclosing passwords, personal data, or granting unauthorized access to systems. This technique commonly exploits trust, fear, and urgency through methods like phishing, pretexting, baiting, and vishing (voice phishing). Social en-

[2] Hacktivism is a form of cyberattack carried out by hackers with political or social motives. They use technical skills to access, damage, or disrupt websites, systems, or networks as a way to voice protests, influence public opinion, or oppose policies considered unfair. Hacktivism can take the form of DDoS attacks (causing access disruption to a site), defacing (altering a website’s appearance), or leaking sensitive information to expose violations. The main goal is to influence social or political change through the power of technology.

[3] Man-in-the-Middle (MITM) attacks are a type of cyberattack in which the attacker secretly infiltrates between two parties who are communicating to steal or manipulate their data. In this attack, the attacker can monitor, modify, or even redirect messages without the victim’s knowledge.

gineering is particularly dangerous because it targets human vulnerabilities rather than technical flaws, making it far more difficult to anticipate and mitigate.

e. Phishing

Phishing refers to a cyberattack in which threat actors disguise themselves as legitimate organizations or individuals to fraudulently obtain sensitive information, including passwords, credit card details, and personal data. Such attacks are commonly executed via email, text messages, or fraudulent websites that mimic authentic platforms, thereby deceiving victims into disclosing confidential information.

f. Attacks on Websites

These are unauthorized attempts to gain access to a website with the intent to alter, steal, insert, or publish malicious content. Examples include defacement (changing the website’s visual appearance or content) and Distributed Denial-of-Service (DDoS) attacks.

g. Seizure of Digital Devices

The physical seizure of digital devices refers to forcibly taking or stealing electronic equipment such as mobile phones, laptops, or other digital tools with the intent to access sensitive data, sabotage systems, or exploit stored information. This threat involves not only the loss of physical devices but also potential digital security risks if the devices lack proper protection, such as passwords, encryption, or tracking features.

h. Gender-Based Digital Attacks

Gender-based digital attacks are cyber incidents targeting individuals based on their gender identity, aiming to degrade, intimidate, or exert control over the victim. Such attacks may include sexual harassment, verbal intimidation, online bullying, the dissemination of private images or videos, and doxing (exposing personal information). Victims, particularly women and gender minorities, are often targeted due to gender inequality and prevailing social stereotypes. These attacks can cause severe psychological harm and threaten victims’ privacy and safety.

i. Digital Threats and Intimidation

A threat refers to any form of communication intended to cause harm to an individual or organization, while intimidation involves coercive or frightening actions aimed at forcing someone to act—or refrain from acting—in a certain way.

Such threats and intimidation are often carried out online to pressure media organizations or journalists into halting coverage that may be unfavorable to certain parties.

CHAPTER III
Definition of SOP

In simple terms, a Standard Operating Procedure (SOP) for Digital Security in Media Companies can be defined as an official company document outlining the steps that everyone within a media organization should follow to prevent and respond to digital attacks.

The term everyone here refers to all personnel across the organization, from the highest level of editorial leadership to the most junior media workers. This is important because, according to research by AJI and PR2Media, digital security SOPs in many media companies are often limited to internal guidelines used only by the information technology (IT) team.

CHAPTER IV
Stages of SOP Development

A well-designed Standard Operating Procedure (SOP) should be developed through a participatory process that involves all members of the media organization. Digital security within a media company is an integrated effort that requires coordinated actions from all parties to ensure comprehensive protection. Therefore, it is essential that personnel at every level, from staff to top management, actively participate in formulating the company's Digital Security SOP.

The following are several steps for developing a Digital Security Standard Operating Procedure (SOP) that media organizations can adopt:

1. **Starting with digital security audit**
   A digital security audit is essential to identify risks, threats, organizational capacity, and employee behavior related to digital security within a media company. This audit can be conducted internally or with the assistance of an external party experienced in performing such assessments. Media organizations that wish to conduct their own audit can refer to the "Digital Security Audit Guide for Civil Society Organizations" developed by SAFEnet.[4] This guide is based on the Security Auditing Framework

[4] Panduan bisa diakses melalui link ini: https://safenet.or.id/id/2024/09/panduan-audit-keamanan-digital-untuk-oms/

and Evaluation Template for Advocacy Groups (SAFETAG), particularly in terms of its content and structure, and has been adapted from SAFEnet's four years of experience conducting audits.

2. **Formation of a Digital Security SOP drafting team**

   Media company leaders can establish a team to draft the "Digital Security SOP for Media Companies." The team may include representatives from various departments, such as information technology, editorial, administration, and legal. A diverse team composition ensures that the SOP draft benefits from multiple perspectives and expertise.

   Company leaders can also formally appoint a coordinator and team members through an official decree. This document provides the team with legitimacy to operate and ensures the necessary budgetary support.

3. **Developing the SOP drafting stages**

   The SOP drafting team can begin its work by holding an initial meeting to discuss the purpose and urgency of creating the Digital Security SOP. This step ensures all members share the same understanding of its importance. Next, the coordinator can facilitate a participatory discussion to develop a work plan, including steps and a realistic timeline. A collaborative approach helps ensure that the process remains feasible and progresses in line with team capacity and expectations.

4. **Review of digital security audit results**

   Before drafting the SOP, the team should study the findings of the digital security audit to identify strengths and weaknesses within the organization. This helps the team design measures in the SOP to address vulnerabilities and minimize risks from digital attacks. The audit results can also serve as a benchmark for the drafting team to assess the organization's capacity and the behavior of people within the media company. Therefore, the team can propose steps to be included in the SOP according to the company's capabilities, including recommendations for organizational culture if there are human behaviors that endanger the company's digital security.

5. Drafting the initial version of the Digital Security SOP

A well-structured Digital Security SOP should include several key components that are clear and easy to understand for all employees. These components typically include background, objectives, scope, principles, prevention mechanisms, response procedures, and monitoring and evaluation systems.

Additional sections, such as key terms, legal foundations, and references, may also be added to improve clarity and usability. This ensures the SOP applies not only to the IT department but also to all levels of the organization in the media company.

6. Presentation of the initial SOP draft

The drafting team should circulate the initial SOP draft to all employees for feedback, either through secure digital communication channels or printed copies. The team should also present the draft to department heads and company executives.

This presentation provides an opportunity to gather insights, refine the document, and discuss any budgetary requirements, such as purchasing licensed software and antivirus protection for employees.

7. Refinement of the SOP draft

The drafting team can revise the SOP based on input from employees and management across departments. Before finalization, the team should conduct a simulation with representatives from different units to ensure the procedures are practical and effective.

Once the SOP has been tested and validated, the team can submit the final version to company leadership, marking the completion of their mandate.

8. Issuance of the official SOP regulation

The company leadership can then formalize the SOP by issuing an "Official Decree on the Digital Security SOP for Media Companies." This provides the SOP with formal authority and ensures it is recognized and followed by all employees.

9. DIssemination and implementation of the Digital Security SOP

Before implementation, the SOP should be introduced and explained to all employees. This dissemination process is crucial to building shared understanding and alignment regarding the new digital security policy.

10. Monitoring and evaluation

The company should appoint supervisors, ideally from the human resources and IT departments, to oversee the implementation of the SOP. These supervisors are also responsible for evaluating their effectiveness and identifying areas for improvement. In most cases, weaknesses in an SOP become apparent only after implementation, making periodic review and revision essential.

CHAPTER V
Components of Digital Security SOP for Media Companies

A well-prepared Digital Security Standard Operating Procedure (SOP) for media companies should include several components that are clear and easy for everyone in the organization to understand. These components typically include the background, objectives, scope, principles, prevention mechanisms, response mechanisms, and monitoring and evaluation systems.

The drafting team may also include additional sections such as key terms, legal foundations, and references to make the SOP easier to understand. This is important because the SOP is not intended solely for the internal IT team but for everyone across the organization, from the lowest to the highest levels.

The following are the key components of a Digital Security SOP that media companies can adopt.

1. SOP Title

The title of the SOP is important to provide a clear explanation at the outset for everyone in the company. For example: “Digital Security Standard Operating Procedure (SOP) for Kabar Batavia Media Company.”

2. Background

The background section outlines the reasons and considerations behind the company's need for a Digital Security SOP. For instance, based on the results of a digital security audit, there may be significant cyber threats and limited organizational capacity to prevent them. Therefore, the company deems it necessary to establish a Digital Security SOP.

3. Objectives

This section describes the goals the media company aims to achieve through the creation of the Digital Security SOP, such as ensuring the protection of data, systems, journalistic works, media content, and confidential information from digital attacks.

4. Scope

The scope defines the coverage or boundaries of activities, processes, and responsibilities outlined in the SOP. For example, it may cover the content management system, editorial and user data, journalistic works, and network access used by the media company.

5. Principles

The following digital security principles can be adopted by media companies in drafting their Digital Security SOP:

A. Data and content security: safeguarding the company's data and content from unauthorized access or cyberattacks.

B. User data protection: media companies must protect users' personal data in accordance with Indonesia's Personal Data Protection Law, including responsibilities for compliance, secure data processing, documentation of processing activities, and confidentiality obligations.[5]

C. Confidentiality: data and information are valuable assets for media companies, particularly in investigative reporting, and must be kept confidential.

[5] https://aji.or.id/system/files/2024-08/modul-pelindungan-data-pribadi.pdf

D. Access control: ensuring that only authorized individuals, based on their job responsibilities, can access company systems.
E. Backup and recovery: regularly backing up data and content to prevent loss of digital assets due to cyberattacks
F. Availability: ensuring adequate human and financial resources are available to maintain digital security, including prevention and response measures.
G. Collaboration and shared commitment: digital security within a media organization requires the collective effort and responsible behavior of all personnel.

6. Prevention Mechanism

The prevention mechanism refers to a series of collective actions taken to establish digital security within the media company. It is essential for everyone in the organization to have a shared understanding of digital security. Companies can organize basic digital security training sessions to align perspectives between staff and management.

Preventive measures against digital attacks should also be detailed in the SOP to serve as a clear reference for all employees. Additional recommended preventive measures can be found in the later sections of this guide.

7. Response Mechanism

The response mechanism consists of procedures carried out by the media company when a digital attack occurs. The response can be handled by internal teams or in collaboration with external parties. For example, if the company's social media accounts are hacked, the response process should involve the relevant digital platform provider.

8. Monitoring and Evaluation Mechanism

All digital activities should be recorded transparently and accountably. This documentation helps the company evaluate the implementation of the Digital Security SOP. In cases of cyber incidents, the company must also document the attacks for collective review and learning.

Equally important is the supervision of the SOP’s implementation. Company leadership may appoint supervisors from the human resources and information technology departments. The findings from monitoring and evaluation can then be used to improve the Digital Security SOP, especially as information technology continues to evolve rapidly.

CHAPTER VI
Prevention and Handling Mechanism

The following steps can be adopted by media companies to prevent and respond to digital attacks. These steps may also be incorporated into the company's Digital Security SOP. However, it is important to note that each media company faces different types and levels of digital threats. Therefore, it is essential for each organization to align its main digital risk areas identified through a digital security audit, with the prevention and response measures outlined in its SOP.

The steps below use technical language that may be easier to understand for staff in the information technology department. Nevertheless, we hope that employees from other departments, as well as company leadership, can gain a general understanding from the explanations provided. We also encourage non-technical staff and management to discuss these steps with the IT department to gain a clearer understanding of the preventive and response measures.

A. Office Network Security

A media organization with a physical office typically requires multiple devices to be connected to a shared network. These devices may include computers, printers, servers, and other tools used by newsroom staff.

At the same time, media offices often have public areasaccessible to visitors or clients. These areas frequently provide internet access, such as public Wi-Fi. However, opening public access, including to the network, can create potential security vulnerabilities. Therefore, it is essential to implement the following measures when managing office networks.

1. Identify network devices
   - Devices may include routers, switches, network printers, Wi-Fi access points, NAS (LAN file storage/file sharing), network projectors, broadband modems, smart TVs, MikroTik routers, domain-connected internet networks, CCTV cameras, and others.
   - Ensure all devices are connected through secure networks and not accessible to the public or outsiders.
   - Keep all devices in secure areas, not exposed to public access.

2. Identify non-networked devices

   Some devices may not be connected to a network but still have storage capabilities—such as photocopy machines, external hard drives, and similar equipment.

3. Network separation
   - Whenever possible, separate internal networks (used by staff for media operations) from public networks.
   - Guest Wi-Fi or public internet access should be isolated from internal systems to prevent unauthorized access to internal resources.
   - Configure the service set identifier (SSID) to distinguish between Wi-Fi networks. SSIDs can be either hidden or public. Hidden SSIDs are not visible to the general public and can only be accessed by authorized

users, while public SSIDs can be visible but secured with a Wi-Fi Protected Access (WPA) password.
- If separation is not possible, avoid offering any external network access.

4. Wi-Fi access management
   - Hide Wi-Fi networks to prevent detection by unauthorized individuals, including those in nearby buildings.
   - Limit access credentials (username and password) to registered and approved devices only.
   - Rename device identifiers from their factory default names (e.g., “DESKTOP****”) to unique labels easily recognized by the network administrator.
   - Understand the risks of allowing public access to the office internet. Individuals with access can identify the network’s IP address. An IP address is the identity of a device connected to the internet or a network. If our device’s IP address is publicly known, it becomes a vulnerability that outsiders can exploit to launch attacks such as injecting malware, tracking location, or performing illegal access.

5. Local Area Network (LAN) management
   If the office uses a LAN connection, ensure access is restricted to internal staff and registered devices. Allowing guest or external devices to connect to the LAN increases the risk of security breaches.

6. Network administrator
   - Designate an internal staff member to serve as the network administrator.
   - If outsourcing LAN or Wi-Fi management to a third party, ensure the provider is reputable, trustworthy, and has no affiliations that could pose a threat to the organization.
   - Keep updated contact information for the third-party administrator and ensure they are reachable when needed.

B. Office Device Security

This section covers all devices owned by the media organization and its staff, including hardware, software, and digital platform accounts. Hardware includes computers, laptops, mobile phones, routers, servers, and similar devices. Software refers to operating systems, programs, and applications used by both the media organization and its employees. Digital platform accounts include social media, messaging applications, email, and other online platforms managed by the organization or its staff.

To ensure the security of these assets, the following measures should be applied:

1. Connected devices
   Ensure that every device connected to the network, whether via a local area network (LAN) or Wi-Fi, is identified and that no unauthorized or unknown devices are connected.

2. Computers and laptops
   - Identify which devices are mobile (such as laptops) and which remain stationary in the office (such as desktop PCs).
   - Place stationary devices, such as PCs, in rooms not accessible to visitors or the public. Mobile devices like laptops must be securely managed by their users.
   - Use only licensed operating systems (OS). Unlicensed or pirated OS versions create unprotected security gaps, leaving devices vulnerable to viruses and malware. Alternatively, open-source operating systems such as GNU/Linux or Ubuntu can be used.
   - Connect only to secure networks, such as office Wi-Fi or LAN, or other trusted private connections. Avoid using public Wi-Fi networks.
   - Consider implementing centralized device management, allowing only IT administrators to install or modify software.
   - Ensure all journalists and staff using company laptops or computers

follow digital security best practices. Detailed guidance are available in Chapter 2 of the Digital Security Guide for Journalists.[6]

3. Routers
   A router connects devices to the internet or other networks and manages data traffic. Place routers in secure areas to protect them from theft, tampering, or physical damage. Hide routers when possible to prevent the office Wi-Fi network from being publicly visible.

4. Surveillance cameras
   - Install surveillance cameras (CCTV) in key areas, such as entry points, document storage rooms, device storage areas, and public spaces within the office.
   - Ensure CCTV cameras are connected only to the internal network, inaccessible to external parties.

C. Website Security[7]

For a media organization, a website is one of the most critical digital assets, serving as the main platform for content distribution and a major source of revenue. Therefore, protecting the website is essential.

Media websites are often targets of digital attacks such as Distributed Denial of Service (DDoS), defacement, or account hijacking. According to AJI Indonesia and PR2 Media's 2024 research, DDoS attacks were the second most common type of cyberattack faced by media organizations in Indonesia. Based on reports collected through advokasi.aji.or.id, out of 16 digital attacks against journalists and media outlets in 2023, three were DDoS cases, three involved website defacement, and one involved website suspension.

Several factors increase a media organization's risk of cyberattacks, such

[6] https://aji.or.id/system/files/2024-07/layoutpanduankeamanandigitaluntukjurnalisfixcompressed_4.pdf

[7] For more details on web security steps, please refer to the link: https://github.com/OpenInternet/ MyWebsiteIsDown/blob/master/MyWebsiteIsDown.md

as the type of information it publishes, potential adversaries (individuals, groups, or institutions with opposing interests), and the organization's resources for web protection.

a. Identifying Threats

One of the most frequent threats to media websites is DDoS attacks. These attacks can make websites inaccessible or slow to load. For media outlets with sufficient anti-DDoS protection, the impact may be minimal, but for those without proper safeguards, the consequences can be long-lasting.

An initial risk assessment helps determine the necessary preventive measures.

1) What needs protection?

Identify the following:

- The types of data or information stored on the website.
- The types of data or information displayed publicly.
- The intended audience of the information.

This identification helps assess the website's vulnerabilities, such as the potential effects of a DDoS attack that prevents administrators and visitors from accessing the site. Based on this, media managers can determine what protection is needed and what steps to take if the website becomes inaccessible.

2) Potential website attackers

It is difficult to identify who might be planning to attack a website. The attackers could be individuals or groups interested in the information shared on the site, and they may change over time.

DDoS and deface attacks may occur alongside sensitive cases or specific events such as elections or the disclosure of a particular case. The following questions can help identify potential threats:

- What kind of content does your media publish?
- Who or what entities are frequently criticized in your reports?
- Who might have interests that conflict with your coverage?
- Who are your competitors?
- Who are your website visitors?
- How influential is your media outlet?

After identifying potential adversaries, consider their motivations and what they might gain from attacking your site.

3) Investment

Assess your organization's readiness to handle website attacks by asking:

- How much budget is allocated for website security?
- What protections are in place to respond to attacks such as DDoS?
- How capable is your technical team in managing web security?

There is no minimum budget standard or single solution for building web protection for institutions or media companies. For large media outlets, web security investments can be quite substantial. Conversely, for media organizations with limited resources, efforts to build protection require a different approach.

- Smaller media organizations can use web hosting providers that include DDoS protection. This option requires minimal technical staff.
- Larger media organizations may hire in-house experts to develop custom security systems.

b. Identifying Attacks (When the Website Is Down)

When a website goes down, several factors may be responsible — coding errors, hosting provider issues, or administrative problems. Identifying the root cause is crucial.

1) Error messages

- An "error" message may indicate a software issue. Check any recent changes made to the site.
- If unresolved, contact the webmaster with a screenshot or description of the error.

2) Messages from the hosting provider

- This may relate to legal or administrative issues such as copyright violations or unpaid hosting fees.
- If copyright infringement is suspected, review any third-party content (text, images, videos, etc.) used on the site.

3) The website does not load at all

- This could be due to hosting provider issues.
- Check the website of the web hosting provider. If the site is experiencing issues or cannot be accessed, it may indicate that the provider is having problems or undergoing scheduled maintenance.
- Check the provider's social media accounts, such as on X or other platforms, or look for information about the provider to see if similar issues are being discussed by netizens.

4) Website unavailable though hosting is normal

- Use http://www.isup.me/ to check whether the issue lies with your site or your connection.
- If the message reads "It's just you," the problem is on your end.

5) Possible censorship

- Try accessing similar sites. If they are also inaccessible, censorship may be the cause.
- Attempt access via Tor, Psiphon, or a VPN. If successful, your site may be blocked domestically.

6) Slow or unstable loading

- If the website loading is unstable—sometimes accessible and sometimes disconnected—or unusually slow, it may be due to a high number of visits or access requests to the site.

- Check the site's traffic, for example through Google Analytics. If there is an increase in visitors but still within a normal range, it indicates a performance issue with your website.
- Contact the webmaster or web hosting provider to improve the site's performance, for example by adding certain plugins.
- Consider using plugins that help with caching (storing data on the server network). Caching can speed up website access and improve performance during high traffic periods.

7) Possible DOS/DDOS

- If the above diagnostics do not identify the exact problem—for example, the site remains difficult to access and performance is still poor—it may be experiencing a Denial of Service (DoS) attack.
- A DoS attack can be carried out by an attacker who repeatedly tries to access a website using automated tools, making it difficult for other users to access the site. If done by a single person, the attack may not cause serious issues.
- However, DoS attacks are commonly executed by an attacker using thousands of machines (Distributed DoS or DDoS) with the aim of paralyzing the website so that legitimate users can no longer access it.

c. DDoS Mitigation

Many services offer protection before, during, and after an attack. Since it can take up to three days to reroute traffic through protected servers, early mitigation is more effective than responding post-attack.

Many services are available to help a website respond to DoS/DDoS attacks. In general, they fall into two categories: hosted services and proxied services.

1) Hosted services

Hosted services require administrators to move their website to the provider's server. Hosting providers usually offer integrated protection, both against DDoS attacks and other types of attacks. However, such services are more expensive (up to around US$500 or Rp8 million per month). In addition, the provider has full control over our website.

a) Advantages:

- Provides centralized protection services.
- Includes other services such as consultations.
- Full support from the service provider.

b) Disadvantages:

- Control of the website is handed over to the service provider.
- Website owners must be careful in choosing a trusted service.
- More expensive.

c) Example of service:

VirtualRoad.org

- Costs start at €100 (around Rp1.7 million) per month. More complex hosting requires higher fees.
- VirtualRoad.org is part of the Media Frontiers project, a social organization from Denmark established by International Media Support (IMS).
- Additional services: website transfer to the provider's system, domain registration, optimization, security audit, protection against hacking and phishing, security report provision related to attack attempts, and legal aspect support.
- Service links: https://virtualroad.org/get-protected/packages and https://virtualroad.org/contact or e-mail info@virtualroad.org.

The Positive Internet Company

- Costs start at $495 (around Rp7.8 million) per month with a fully managed server (full served server) for a website. Another option is shared hosting priced at £125 (around Rp2.6 million) per year.
- The Positive Internet Company is a nonprofit organization based in the United Kingdom and the United States.
- Additional services: firewalls, database management, and backup.

- Service links: http://www.positive-internet.com/services/vip-hosting and http://www.positive-internet.com/contact-us or e-mail good@positive-internet.com.

2) Proxied services

Proxied services can be an option if administrators want to retain control and host their own website, making configuration easier. Service providers have many servers in various parts of the world that protect websites from abnormal traffic. This protection is carried out by mirroring and presenting an updated copy of our website.

a) Advantages:

- Lower cost (some start at the free level).
- Faster and easier configuration.
- No need to change the website hosting.
- Option to stop the service at any time.

b) Disadvantages:

- Limited support beyond protection against DDoS attacks.
- Few additional services such as anti-malware or anti-spam.
- Data traffic encrypted through Secure Socket Layer (SSL), also known as HTTPS, can be decrypted and re-encrypted by the proxy server. If the data traffic is decrypted, it creates a potential vulnerability for attackers.

c) Example of service:

Deflect

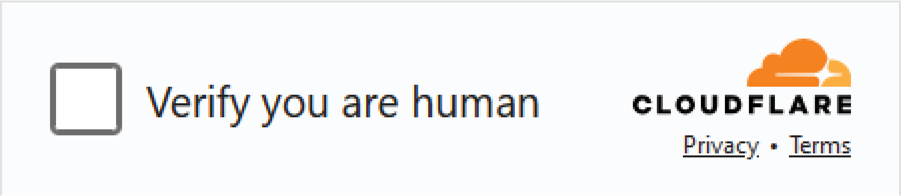
- Free of charge.
- Intended for websites owned by NGOs, human rights defenders, and independent media.
- Deflect is an open-source project by eQualit.ie, a nonprofit technology collective based in Montreal, Canada. Deflect is funded by NGOs and governments of several countries, including the United States, to protect freedom of expression. Deflect does not

publicly disclose which websites it protects and does not require approval to provide its services.

- Additional service: the Deflect team has several grants to fund additional SSL certificates and other protection costs.
- Service links: https://wiki.deflect.ca/signup/ or https://wiki.deflect.ca/wiki/Join_Deflect.

CloudFlare

- Cost: free for the basic level, $20 per month with additional SSL support, and $200 per month for higher needs.
- There are restrictions on service recipients based on U.S. foreign policy (see https://blog.cloudflare.com/thoughts-on-abuse).
- Cloudflare is a service from a San Francisco-based for-profit company. Cloudflare protects servers around the world and is subject to the legal regulations of several countries.
- Cloudflare is widely used by various websites, from major media such as The New York Times and BBC to several national media sites in Indonesia.
- Service link: https://www.cloudflare.com/sign-up.



Google's Project Shield/PageSpeed

- Cost: PageSpeed is free during the trial period; Project Shield is offered for free to trusted testers.
- Service users must obtain approval (within 2 hours). Some organizations or countries may face restrictions. Project Shield, on the other hand, can only be used by invited organizations and only accepts requests from websites containing news, human rights, or election-related content.

- The service is provided by Google Inc., which is subject to the laws of certain countries, including the United States.
- PageSpeed link: https://developers.google.com/speed/pagespeed/service.
- Project Shield link: http://projectshield.withgoogle.com/about/.

d. Data Backup

Regular data backups are very important in mitigating DDoS attacks. When a website goes down due to a DDoS attack, administrators can restore data by importing backup data stored on a separate system.

1) Hosted Service

There are two ways to back up website data using a hosted service: exporting data from all pages, posts, and comments into an XML file, and creating a mirroring website (a copy of the main website hosted on another server).

An XML file only contains data in text form and cannot create copies of image files or other media. To ensure the website has a proper backup, it is necessary to create a mirroring website, which is a replica of the website on another server.

2) Shared Hosting

Administrators can copy all files from the website and save a snapshot of the site's database.

3) Web Server Milik Sendiri

Administrators with their own servers must be able to perform automatic backups to a separate server.

D. Communication Security

1. Using Encrypted Messaging Applications
   a. Use messaging applications that provide end-to-end encryption, which means that only the communicating users can read the messages.

b. Avoid using WhatsApp for high-risk communications. Although it claims to use end-to-end encryption, WhatsApp remains vulnerable to attacks due to its popularity and several past hacking incidents.
c. Use alternative messaging apps that include features such as self-destructing messages, such as Telegram, Signal, or Wire.
d. Disable automatic backup, especially when using messaging apps for high-risk communications.
e. Consider using multiple messaging platforms to separate different types of communication.

2. Monitoring Communication Security
   a. If the editorial team continues to use WhatsApp, make sure the security notifications feature is enabled.
   b. On WhatsApp, activate “security notifications” by going to Settings - Account - Security, and ensure “Show security notifications on this device” is checked.
   c. Chats that are end-to-end encrypted between you and another user have their own security code used to verify that the calls and messages you send in that chat are end-to-end encrypted.
   d. This code can be found in the contact info screen as both a QR code and a 60-digit number. Each chat has its own unique code that can be compared with the contact’s code to verify encryption.
   e. If security notifications are enabled, users will be notified when a contact’s security code changes.
   f. Pay attention if there is a notification of a security code change on our contacts. Notifications may appear when:
      - The contact reinstalls WhatsApp.
      - The contact changes their phone device.
      - The contact adds or removes a linked device.
   g. These notifications can be a warning that a contact’s account may have been taken over.
   h. On Signal, there is a safety number. Each private chat on Signal has a unique safety number that allows users to verify the security of their messages and calls with a specific contact.

i. Similar to WhatsApp, the safety number can be viewed in the contact info as a QR code and a 60-digit number:
   - Open the chat with your contact.
   - Tap the three-dot menu and select “Conversation settings.”
   - Choose “View safety number.”

j. Signal will notify you if your contact’s safety number changes, allowing you to check whether your communication is still private.

k. If a contact switches to a new phone or reinstalls Signal, you will receive a notification about the safety number change.

l. If a contact’s safety number changes repeatedly or unexpectedly, verify the contact’s identity directly.

3. Choosing and Managing Browsers

a. Use browsers that prioritize user privacy, such as Firefox or Brave. Some browsers collect user activity data, including browsing history, keywords, IP addresses, and location.

b. Adjust browser settings to limit the amount of personal data recorded. You can compare browser privacy levels at https://www.mozilla.org/en-US/firefox/browsers/compare/.

c. Privacy settings for Chrome are at chrome://settings/privacy, and for Firefox at about preferences#privacy. Review what digital traces are being stored and decide whether you want to allow them.

d. Regularly clear browsing history and cached activity data.

e. Never store sensitive information such as passwords or credit card numbers in the browser.

f. Set browsers to log you out automatically from all accounts when closed.

4. Ensuring Website Protocol Security

a. Make sure that websites you access use the https protocol (Hypertext Transfer Protocol Secure) instead of http.

b. Do not enter usernames or passwords on sites that still use http, especially for emails, social media, or online banking.

5. Adding Security Plugins or Add-ons

   There are several plugins or add-ons that can enhance security and provide alerts when suspicious activity occurs while you are communicating over the internet.

   a. Privacy Badger is useful for identifying which applications track your activity when visiting certain websites. Add the Privacy Badger add-on for Mozilla at https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/. For Chrome, add it from https://chrome.google.com/webstore/detail/privacy-badger/pkehgijcmpdhfbdbbnkijodmdjhbjlgp.
   b. HTTPS Everywhere is useful for encrypting website protocols that do not yet use HTTPS. For Mozilla, add it from https://addons.mozilla.org/en-US/firefox/addon/https-everywhere/, and for Chrome, from https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=en. Alternatively, Mozilla users can set their browser to access only HTTPS sites by enabling HTTPS-Only Mode in about:preferences#privacy without installing any plugins.
   c. Cookie AutoDelete is useful for deleting cookies (digital trace residues) as soon as you close the browser. For Chrome users, add it from https://chrome.google.com/webstore/detail/cookie-autodelete/fhcgjolkccmbidfldomjliifgaodjagh?hl=en. For Mozilla users, add it from https://addons.mozilla.org/en-US/firefox/addon/cookie-autodelete/.

6. Secure File Sharing

   Use file-sharing services that prioritize security instead of Google Workspace. Alternatives include:

   a. For collaborative document editing: www.cryptpad.fr
   b. For sharing large files: https://send.tresorit.com/
   c. For general file sharing: www.mega.nz

7. Masking Communication Traces with VPN

   a. Use a Virtual Private Network (VPN) when accessing public Wi-Fi in cafes, hotels, airports, or when you must visit HTTP sites.

b. Public Wi-Fi, such as those found 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 easily be intercepted by malicious third parties. A VPN encrypts your internet connection, keeping your data secure even when using unsecured public Wi-Fi networks.

c. Avoid unreliable or free VPN services that may collect personal data or request excessive access permissions. Safer options include Proton VPN and Mullvad.

d. If a paid VPN is not possible, use a trustworthy free VPN such as Proton VPN, which offers strong protection and operates under Swiss privacy laws. Free versions may have limited server choices but offer unlimited access and bandwidth.

8. Choosing a Secure Email Service

a. Use email providers that support encryption, such as RiseUp, ProtonMail, Disroot, or Tutanota.

b. Add encryption to corporate email accounts using PGP-Key or Enigmail on the Thunderbird email client.

c. Add encryption functionality to unencrypted email services using browser extensions such as Mailvelope.

9. Checking Attachments and Links

a. If you receive emails with links or attachments from unknown senders, do not open them immediately. It's possible that the link or attachment contains malware that can infect your laptop or smartphone. Malware can spy on your activities (spyware) or steal data from your device.

b. Scan suspicious links or attachments using online tools such as https://urlscan.io/ or https://www.virustotal.com/gui/home/upload.

10. Using Safe Search Engines.

a. Use search engines that do not record your search history, such as DuckDuckGo (https://duckduckgo.com/), StartPage (https://www.startpage.com/), or Qwant (https://www.qwant.com/).

11. For more detailed communication security guidelines, see Chapter 4 of the Digital Security Guide for Journalists.[8]

[8] https://aji.or.id/system/files/2024-07/layoutpanduankeamanandigitaluntukjurnalisfixcompressed_4.pdf

CHAPTER VII
Handling Mechanism

There are several actions that should be taken when a media organization or journalist becomes the target of a digital attack or realizes they are under threat.

1. **Do not panic. Stay calm before responding to the attack.**
   A panicked reaction can worsen the situation and lead to rash decisions, such as disclosing sensitive information, clicking on malicious links, or taking actions that exacerbate the damage. By remaining calm, you can assess the threat more objectively and take well-considered steps to respond to the attack, such as disconnecting from the internet, changing passwords, or reporting the incident to the authorities or professionals. Maintaining emotional control also allows for a more efficient and effective response to prevent or mitigate the impact of a digital attack.

2. **Take emergency steps to identify the problem**
   The following emergency measures can help identify and limit the impact of a digital attack:
   1. Disconnect from the internet: Immediately unplug or disable your internet connection to prevent further spread or damage.

2. Check for suspicious activity: Review unusual activities on your devices or accounts, such as unfamiliar logins, setting changes, or missing or newly appearing files.
3. Run a security scan (antivirus): Use updated antivirus or security scanning software to detect malware or viruses on your device.
4. Change passwords: Reset passwords for any accounts linked to the compromised device and enable two-factor authentication (2FA).
5. Review log history and activity: For online accounts or applications that remain accessible, check login and activity histories for signs of unauthorized access.
6. Back up important data: Immediately back up safe and intact data to prevent further data loss.Immediately back up safe and intact data to prevent further data loss.
7. Contact service providers or cybersecurity professionals: If needed, reach out to qualified cybersecurity professionals or civil society organizations capable of handling cyberattacks (such as the Fast Response Team or TRACE) for assistance and remediation.
8. Report the attack: Notify the application or platform provider for account recovery, or report the incident to the police if necessary.

3. **Document the condition of your account**
   - Record the contents of any messages (emails or direct messages), notifications, or other warning signs.
   - The easiest documentation method is to take screenshots and store them securely as evidence.

4. **Create a chronology of the incident**

   This step can be challenging during stressful moments. Take a moment to calm yourself, then reflect on when the first signs of unusual digital activity appeared, when access was lost, and what actions were taken in response. Use a notepad or digital tool to record these details chronologically.

   The followings are the initial emergency steps to respond to an attack:

   A. **Website Attack**

   To respond to an attack targeting the organization's website, refer back to Chapter VI (Prevention and Response Mechanisms), Part C

(Web Security), Subsections b (Identifying Attacks) and c (DDOS Attack Mitigation) in this guide.

B. Loss of Access to Accounts

Email, social media, and messaging platforms are vital channels for media organizations to distribute journalistic content, including reports on sensitive issues. For this reason, these accounts are highly likely to become targets of digital attacks.

One possible impact of such attacks is the loss of access to a digital platform account. If this happens, make sure to take the following steps:

1. Identification of Problem

a. Ensure that the username and password you entered are correct, with no typos, including the position of the caps lock.
b. Recall the last time you changed your password and try entering your most recently created password.
c. Check the latest admin access (if there is more than one admin). Ensure that no admin has deleted the account. If the account has been deleted (either by an admin or someone else), it cannot be recovered.
d. Check whether you can still access the email account and phone number associated with the account (recovery email and number).
e. Check your email inbox for any notifications indicating login attempts from unfamiliar devices.
f. If the issue involves a social media account, view your profile (through another account or search engine) to see whether anything has changed or if there are posts you never made.
g. If any posts have disappeared, new posts appear that you did not upload, you receive notifications of logins from unknown devices, or there are signs that your recovery email or phone number has been changed without your action, your account has likely been taken over by someone else.
h. If the username and password are correct, your account may have been blocked or suspended by the platform. This can

happen if your account was mass-reported by other users or deemed to have violated the community guidelines.

2. WhatsApp Hacking

a. Confirm whether your WhatsApp account was actually hacked. If you're suddenly logged out, it may indicate an attempt to access your account from another device.

b. If your WhatsApp only logs out but hasn't sent messages to others, the attacker likely hasn't gained full access because a PIN is still required (if you enabled Two-Step Verification).

c. If your account has already sent messages to others, the attacker has likely taken control of it and may have activated 2FA.

d. Follow these steps:
   - Uninstall WhatsApp and reinstall it.
   - Register your number and wait for the SMS verification code (6 digits). If you don't receive the SMS, wait and try again after 10 minutes.
   - If the timer expires, select the "Call me" option to receive the verification code via phone call.
   - When you receive a call, an automated voice will tell you a 6-digit verification code. Enter this code to verify your WhatsApp account.
   - Once your account is recovered, immediately add a PIN and email address to prevent your WhatsApp account from being stolen again.
   - If you still have trouble logging in and are asked to enter a two-step verification code, the hacker may have activated a PIN on that WhatsApp account. You will need to wait 7 days before you can access the account without the two-step verification code.
   - Report that your account has been stolen by emailing support@whatsapp.com with the subject line "Lost/Stolen: Please deactivate my account" in the email body.

3. Gmail Account Hacking

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

b. If you can't log in, open the account recovery page by clicking the link https://s.id/PemulihanGmail. You will be asked to enter your recovery account and follow the instructions to regain access to your email account.

c. For more details on Gmail account hacking and recovery, you can follow the steps in this link: https://support.google.com/accounts/answer/7682439?hl=id.

4. Yahoo Mail Hacking

a. Reset your password by visiting https://help.yahoo.com/kb/SLN27051.html.
b. Enter your Yahoo Mail account email address.
c. Choose your preferred reset method — via phone number or recovery email that you have registered. Recovery via email is recommended over phone number.
d. A code will then be sent to your recovery email or via SMS. Enter that code on the Yahoo page.
e. Create a new, stronger password using a combination of numbers, letters, and spaces.

5. Facebook Account Takeover

a. To find out whether someone else has secretly accessed your account, go to Settings - Security and Login Info, then check “Where You’re Logged In” to see the list of devices (laptops or phones) that have accessed your account.
b. If you find a device that doesn’t belong to you, click the three dots on the right and select Log Out. Change your password to a stronger one.
c. When your account has been hacked and the password has been changed, Facebook will send a notification to your registered email. Check whether you’ve received such a notification.
d. In the notification email, Facebook provides a “Click here” link for users who did not make the password change. The link will direct you to answer Facebook’s verification questions to recover your account.
e. To report a hack, go to https://www.facebook.com/hacked.

6. Instagram Account Takeover

a. If you’re using a laptop, you can check whether someone else has secretly accessed your account by going to Settings □ Login

Activity. This page will display information about the type of device and login location

b. If you find a device you don't recognize, click the arrow on the right, then select Log Out.
c. If you can no longer access your Instagram account, check the notification email sent to your registered address. Instagram sends alerts for any changes made to your account, such as logins from different devices or password changes.
d. Click the Secure Your Account Here feature, and you'll be directed to a page where you can change your password. Enter a new, stronger, and unique password.
e. If your account is difficult to recover, report it to Instagram by following these steps:
   - 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 to enter a secure email address that only you can access. After submitting your request, wait for an email from Instagram containing the next recovery steps.

7. TikTok Account Takeover

a. If you experience the following issues with your TikTok account, it may be a sign of hacking:
   - Your account password and linked phone number have been changed.
   - Your username or nickname has been altered.
   - Videos you've uploaded are deleted, or new videos appear without your consent.
   - Your account sends messages without your knowledge
b. TikTok's official page does not provide detailed procedures for account recovery. However, you can try the following steps based on TikTok's available security features:
   - Open the TikTok app on your phone and select “Forgot password.”
   - You will be asked to enter the contact information linked to your account (phone number or email), depending on the

recovery method you set up when creating the account.
- Tap "Reset" to receive a recovery code. The code will be sent to your phone (via SMS) or email.
- Enter the code in the recovery or "forgot password" menu. If everything works properly, you can change your password to a new, stronger one.
- If the process succeeds, at least the hacker won't know your new password. Strengthen your account security with a stronger 2FA (two-factor authentication), such as using a physical passkey if available.

c. Remove suspicious connected devices[9]
- Check whether your TikTok account is logged in on other devices.
- Open the "Settings and Privacy" menu, then select "Security." Click "Select your devices."
- Remove all other suspicious devices.
- Account strengthening and device removal steps can also be accessed through the "My account has been hacked" page on TikTok's official website.

d. Report the hacking to the platform provider
You can find the steps for reporting problems to TikTok on the Report a Problem page at https://support.tiktok.com/en/log-in-troubleshoot/troubleshooting/report-a-problem.

e. Seek help if recovery fails
- Stay calm and outline the chronology of the hacking incident.
- Document all signs of hacking (notifications, email alerts, and recovery steps), for example by taking screenshots.
- Contact emergency support services for assistance (the list of emergency contacts can be found at the end of this guide).

8. YouTube Account Takeover

Every YouTube account is connected to a Google account. However, there have been cases where a hacked YouTube account could not be restored even though the Gmail account had already been recovered.

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

In 2022, a YouTube account belonging to a gender minority activist group was hacked. The hacker easily took over the account because the password was simple (easy to guess) and rarely changed.

Recovery efforts were made by forcing access into the Gmail account linked to the YouTube account, which was successfully regained. However, the YouTube account itself could not yet be restored. After several recovery attempts, the YouTube account was deleted.

An email from YouTube appeared, informing that the account had been deleted for violating the rules. They repeatedly filed appeals using the link provided in the email, but YouTube stated that the account was no longer registered. The account was finally restored after the case was reported to Google with assistance from an organization experienced in handling digital attacks.

a. Identifying Signs of Hacking
   - Changes appear on your account that you did not make. For example, modifications to your profile picture, description, e-mail settings, AdSense, or messages sent without your knowledge.
   - The account uploads videos you never created. This means someone else has uploaded videos using your Google account. Check if there are e-mail notifications warning you about unfamiliar video uploads or login activities from another device.

b. Account Recovery[10]
   1) Recovering a Google/Gmail Account
      - If you can still log in to your Google account, immediately change your password to a stronger one and enable 2FA (using an authenticator app or physical passkey).
      - If you cannot log in to your Google account, follow the account recovery steps described in point 3 of this section.

[10] Google, “Recover a hacked YouTube channel”, https://support.google.com/youtube/answer/76187?hl=en

- Perform the same steps for any other Google accounts you have.

2) If the Google account can be secured, the YouTube account should also be recoverable.
3) Detailed steps for account recovery can be found on the page Recover a hacked YouTube channel.

c. Seek Help if Recovery Fails
- Stay calm and create a timeline of the hacking incident.
- Document all signs of hacking (notifications, e-mail alerts, and recovery attempts), for example, by taking screenshots.
- Contact emergency support for assistance (a list of emergency contacts can be found at the end of this guide).

d. Restore the YouTube Channel to Its Pre-Hack State[11]

Jika peretas sempat mengambil alih *channel* Youtube, biasanya mereka membuat beberapa perubahan pada *channel* tersebut dan akun Google yang terhubung.

1) Document all traces left by the hacker on the YouTube channel, including the connected e-mail account. One way to do this is by saving them on archiving websites such as https://perma.cc/ or https://archive.is/.

2) Remove all users connected to the compromised YouTube channel.
   - If using "channel permissions," sign in to YouTube Studio. Click "Settings," then "Permissions." Select the username to remove and click "Remove access."
   - If using a "brand account," go to the "Brand Accounts" section under your Google Account settings and follow a similar removal process.

[11] 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

3) Restore the channel to its original settings.
   If the hacker changed the channel name, profile picture, or banner, revert them to their original state to avoid permanent deletion of the account.

4) Permanently delete any videos uploaded by the hacker.

5) 5) Detailed recovery and channel restoration instructions can be found on the page Clean up a hacked YouTube channel.

C. Buzzer Attacks

Buzzer attacks can take various forms, including trolling (creating chaos through comments, arguments, or false information to provoke negative reactions), doxing (exposing a targeted person's private information), impersonation (account forgery or identity theft), and online gender-based violence (OGBV).

The following are several response measures adapted from Chapter 6 of the Digital Security Guide for Journalists 2022:

a. *Doxing*
   - If a journalist's home address is exposed, the media organization should arrange a temporary safe house for the affected person and their family until the situation subsides.
   - Report posts containing doxing to the platform and block the perpetrator's account.
   - If the perpetrator discloses the victim's phone number and the victim receives numerous harassing calls or messages, the phone should be turned off temporarily, and consider changing the number later.
   - If the perpetrator exposes the victim's bank account, credit card, or other financial information, immediately contact the relevant financial institutions and report the breach.
   - Temporarily deactivating social media accounts may be the best option if the attack escalates.
   - Report the doxing incident to the police, bringing documentation and relevant links as evidence.
   - Archive evidence using websites such as https://perma.cc/ or https://archive.is/.

b. Impersonation
  - Issue a public announcement regarding the fake account to prevent audiences and followers from being misled.
  - Report accounts impersonating your media organization or its journalists to the respective platform so that the fake accounts can be removed.
  - Report fake accounts through the following links:
    - Facebook: https://s.id/akunpalsuFB
    - Twitter/X: https://help.x.com/en/forms/authenticity/impersonation
    - Instagram: https://s.id/akunpalsuIG
    - Gmail: https://s.id/akunpalsuGmail

c. Online Harassment and OGBV (Online Gender-Based Violence)
  - Report and block any accounts, posts, or comments containing harassment, including OGBV, on the relevant platforms.
  - Seek support from professional organizations or institutions that provide assistance for victims of harassment or sexual violence.
  - Report incidents of harassment or violence to the police, whether they occur via phone, text, chat, or social media, and include relevant documentation as evidence.
  - The media organization should facilitate trauma recovery services for journalists who are victims of such attacks.

CHAPTER VIII
Digital Security Guidelines of Other Organizations

Media organizations can also study and adopt digital security guidelines published by other institutions. These should, of course, be adjusted to meet each organization's specific needs. The following are examples of digital security guides from other organizations that can help strengthen a media company's own digital security framework.

1. https://gijn.org/digital-security/
2. https://cpj.org/2019/07/digital-safety-kit-journalists.php#protect
3. https://digitalrightswatch.org.au/2019/06/10/digital-securityforjournalists/
4. https://cpj.org/2020/05/digital-safety-protecting-againsttargeted-onlineattacks/
5. https://coconet.social/digital-hygiene-safety-security-indonesia/
6. https://freedom.press/training/your-smartphone-and-you handbookmodern-mobilemaintenance/
7. https://www.accessnow.org/issue/digital-security/
8. https://digitalfirstaid.org/en/index.html
9. https://securityinabox.org/en/guide/basic-security/android/

10 https://id.safenet.or.id/wp-content/uploads/2019/11/PanduanKBGO-v2.pdf

11. https://digsec.safenet.or.id

CHAPTER IX
Emergency Contacts

A. Technical Assistance Contacts

In the event of an attack or when media organizations 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

Institution	Address	Phone	Fax	Email
LBH Pers	Jl. Kalibata Timur IV G No.10 Kalibata, Pancoran, Jakarta Selatan	021-79183485, 0821-4688-8873		secretariat@l bhpers.org
YLBHI	Jl. Diponegoro No.74, Menteng, Jakarta Pusat 10320	021-3929840	021-31930140	info@ylbhi.or.id
LBH Jakarta	Jl. Pangeran Diponegoro No.74, Menteng, Jakarta 10320	021-3145518	021-3912377	lbhjakarta@bantuanhukum.or.id
PBHI	Jl. Hayam Wuruk No.4, RT.9/RW.5, Kb. Klp., Kec. Taman Sari, Jakarta 10120	021-3859968		
LBH Apik Jakarta	Jl. Raya Tengah No. 31 RT01 RW09 Kampung Tengah Kramat Jati Jakarta Timur 13540	021–87797289, 0813-888226699	021–87793300	LBHAPIK@gmail.com

West Java and Banten

Institution	Address	Phone	Fax	Email
LBH Bandung	Jl. Kalijati Indah Barat No 8, Antapani, Bandung	0821-2017-1321		konsultasi@lbhbandung.or.id
LBH Apik Jabar	Jl. Beringin No.9 Kemiri Muka, Beji, Kota Depok, Jawa Barat	0813-8030-4852		lbhapikjawabarat@gmail.com
LBH Apik Banten	Jl. Raya Pandeglang Km. 3, Komp. Tembong Indah, Sempu, Kota Serang – Banten	0254-227969	0254-227969	

Central Java and Yogyakarta

Institution	Address	Phone	Fax	Email
LBH Semarang	Jl. Jomblangsari 4 No. 17, Jomblang, Candisari, Kota Semarang	024-86453054, 0882-2890-2001		office.lbhsemarang@ylbhi.or.id
LBH Apik Semarang	Jl. Poncowolo Timur Raya No. 455 Semarang,Jawa Tengah (masuk melalui jalan Indraprasta)	024-3510499	021-31930140	apiksemarang@yahoo.com
LBH Yogyakarta	Jl. Benowo No.309, Winong, RT 12/ RW 03, Prenggan, Kec. Kotagede, Kota Yogyakarta, Daerah Istimewa Yogyakarta 55172	0274-4351490	021-3912377	kalabahulbhjogja@gmail.com
LBH Apik Yogyakarta	Jl. Nogodewo 12, Gowok, Sleman, Yogyakarta	0274-379614, 08179410624	021–87793300	apik_jogja@yahoo.com

East Java

Institution	Address	Phone	Fax	Email
LBH Surabaya	Jl. Kidal No.6, Pacar Keling, Kec. Tambaksari, Kota SBY, Jawa Timur 60131	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	081252226205		lbhmalang@ylbhi.or.id
LBH APIK-Kota Batu	Jl. Kapten Ibnu, Ruko 8 RT03/ RW13, Kel Sisir, Batu, Kota Batu, Jawa Timur	6281336554420		lbhapikkotabatu@gmail.com

Bali and Nusa Tenggara

Institution	Address	Phone	Fax	Email
LBH Bali	Jl. Plawa No.57, Denpasar Timur, Denpasar, Bali	0361-223010		lbhbali@indo.net.id
LBH APIK Bali	Jl. Suli 119 – A3, Denpasar Timur	0361–9272245, 081337325896		lbh.tentrem@gmail.com
LBH APIK NTT	Jl. Sam Ratulangi II no.33B Walikota Baru, Kel. Oesapa Barat, Kec. Kelapa Lima, Kota Baru, Kupang 85228.	0380 823647		lbhapik.ntt@gmail.com
LBH APIK NTB	Jl. Angklung Raya no. 2 Karang Bedil, Mataram, Lombok, NTB	0817-5768-496, 0823-3959-3221		lbhapikntb17@gmail.com

Aceh and North Sumatera

Institution	Address	Phone	Fax	Email
LBH Banda Aceh	Jl. Sakti Lorong LBH Banda Aceh No.1, Desa Pango Raya, Ulee Kareng, Banda Aceh 23119	0651-8057952		lbh_aceh1995@yahoo.com
LBH APIK Aceh	Jl. Tengku Daud No. 147, Panggoi, Muara Dua, Kota Lhoksmeumawe, Aceh 24355	0645-43150		lbhapikaceh@gmail.com
LBH Medan	Jl. Hindu No.12 Medan 20111, Sumatera Utara, Indonesia	061-4515340	061-4569749	lbh_medan@ yahoo.com, kantor@lbhm edan.org
LBH APIK Medan	Jl. Jermal V No. 1C, Denai, Medan Denai	0821-5753-9308, 0282-115063359		admlbhapikm edan@gmail.com

Wilayah Sumatera Barat dan Riau

Lembaga	Alamat	Telepon	Faks	Email
LBH Padang	Jl. Pekanbaru No 11A, Kota Padang, Sumatra Barat	0751-7056059		
LBH Pekanbaru	Jl. Sapta Taruna No.51, Tengkerang Utara, Kec. Bukit Raya, Kota Pekanbaru, Riau 28289	0761-45832, 0811-765-832		info@lbhpeka nbaru.or.id

South Sumatera and Lampung

Institution	Address	Phone	Fax	Email
LBH Palembang	JL. HBR Motik No.12A Rt.29 Rw.9 Kel.Karya Baru Kec. Alang-alang Lebar Kota Palembang	0711-5610122, 0813-6930-0442		lbhpalembang@ylbhi.or.id
LBH APIK Sumatera Selatan	Jl. Sekip Bendung Dalam No.009 RT. 035 RW. 009, Kel. 8 Ilir, Kec. Ilir Timur III, Kota Palembang	0821-7770-0069		yayasanlbhapiksumsel@gmail.com
LBH Bandar Lampung	Jl. Sam Ratulangi, Gg Mawar 1, Nomor 7, Gedong Air, Bandar Lampung 351117	0721-5600425		bantuanhukumlampung@gmail.com

Kalimantan

Institution	Address	Phone	Fax	Email
LBH Kalimantan Barat	Jl. Dr. Sutomo, Komplek Batara Indah 4 No. 16 D, Pontianak, Kalimantan Barat	0812-5880-6816		lbhkalbar@ylbhi.or.id
LBH APIK Pontianak	Jl. Alianyang No. 12A Pontianak, Kalimantan Barat 78116	0561–766439		apik_ptk@ya hoo.com
LBH Samarinda	Jl. Wijaya Kusuma II No 50, Air Putih, Samarinda Ulu Samarinda	0821-5133-15537		lbhsamarinda @ylbhi.or.id, lbhsamarind @gmail.com
LBH APIK Kalimantan Timur	Jl. Sultan Sulaiman, Perum Citra Gading Blok B2 No. 9 Samarinda – Kalimantan Timur	0541-4106482, 0812-5822-715, 0812-5826-828		ylbhapikkalti m@gmail.com
LBH Palangka Raya	Jl. Parawei, Perum Casadova blok B, No. 10, Kota Palangka Raya, Prov. KalimantanTengah	0857-8696-8317		ylbhi.lbh.palangkaraya@gmail.com

Sulawesi and Papua

Institution	Address	Phone	Fax	Email
LBH Manado	Jl. A Manonutu No. 29, Wanea, Kota Manado 95116	0431-8806473, 085256303949, 085240523068		secretariat@l bhpers.org
LBH APIK Manado	Jl. Bethesda 6 No. 77, Ranotanaling II, Manado - 95116	0431-824132	021-31930140	info@ylbhi.or.id
LBH Makassar	Jl. Nikel 1 Blok A22 No.18 Kota Makassar, Kode Pos 90222	0411-4677699	021-3912377	lbhjakarta@bantuanhukum.or.id
LBH APIK Makassar	Jl. Perintis Kemerdekaan, Perum Budidaya Permai Blok D no. 3, Makassar, Sulawesi Selatan			
LBH APIK Palu	Jl. Teluk Tomini No. 8B, Kota Palu - 94221	0451-4015986, 0811-4540-1616	021–87793300	LBHAPIK@gmail.com
LBH Papua	Jl. Gerilyawan No. 46 Jayapura, Papua 99532	0967-581710, 08124808635		
LBH APIK Jayapura	Jl. Raya Sentani, Padang Bulan, Abepura, Jayapura, Papua 99351	0411-590147, 0812-9400-7696		

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 nationwide