ODLAN

# Digital Incident Response Strategy

(Name of Organization)

(Date of Last Update)


| | |
|---|---|
| **1. Crisis Response Plan for Online Threats** | **2** |
| **2. Social Media Account Dogpiling** | **5** |
| **3. Social Media Account Cloning (Instagram)** | **9** |
| **4. Social Media Account Hacked** | **13** |
| **5. Website Attack** | **17** |
| **6. Email Phishing** | **22** |
| **7. Doxxing (Personal Information Leaked)** | **24** |
| **8. Self-Care Recommendations for After Being Doxxed** | **27** |
| **References** | **29** |


**Section 1 is a general crisis response framework that applies to all online threats.**

**Sections 2-8 are specific use cases that provide detailed guidance for each incident type. Start with Section 1 for the overall response, then refer to the relevant specific section for tailored steps.**

ODLAN

# 1. Crisis Response Plan for Online Threats

## 1.1. Purpose

The purpose of this Crisis Response Plan is to provide a structured approach for handling threats to social media accounts. This plan aims to mitigate risks, protect the organization's reputation, and ensure a coordinated response to any threat that impacts social media channels.

## 1.2. Scope

This plan applies to all social media accounts managed by the organization or individuals. It covers all types of threats, including security breaches, misinformation, harassment, and targeted attacks.

## 1.3. Crisis Response Team (CRT)

### 1.3.1. Team Composition

- **Crisis Manager:** Responsible for overseeing the response and making strategic decisions.
- **Social Media Manager:** Handles the immediate response on social media platforms and content moderation.
- **IT Security Specialist:** Manages technical aspects, including security breaches and account recovery.
- **Public Relations Officer:** Coordinates external communication and manages the organization's public image.
- **Legal Advisor:** Provides guidance on legal implications and regulatory compliance.
- **HR Representative:** Supports affected employees and manages internal communication.

### 1.3.2. Contact Information

- **Crisis Manager:** [Name, Contact Information]
- **Social Media Manager:** [Name, Contact Information]
- **IT Security Specialist:** [Name, Contact Information]
- **Public Relations Officer:** [Name, Contact Information]
- **Legal Advisor:** [Name, Contact Information]
- **HR Representative:** [Name, Contact Information]

## 1.4. Incident Detection and Assessment

#### 1.4.1. Detection

- **Monitoring Tools:** Use social media monitoring tools to detect unusual activity or threats.
- **Employee Reporting:** Encourage employees to report any suspected threats or unusual activity on social media.

#### 1.4.2. Assessment

- **Initial Evaluation:** Assess the nature and scope of the threat, including the type of threat (e.g., security breach, misinformation, harassment) and its potential impact.
- **Severity Rating:** Categorize the threat based on its severity (e.g., low, medium, high) to prioritize response actions.

### 1.5. Immediate Response Actions

#### 1.5.1. Containment

- **Isolate Threat:** Take immediate steps to contain the threat, such as disabling compromised accounts, removing harmful content, or restricting access.
- **Secure Accounts:** Implement additional security measures, such as changing passwords, enabling multi-factor authentication, and reviewing account permissions.

#### 1.5.2. Communication

- **Internal Notification:** Notify the Crisis Response Team and relevant internal stakeholders about the threat and initial response actions.
- **External Communication:** Prepare a holding statement to acknowledge awareness of the issue and that a response is being developed. Avoid detailed disclosures or speculations at this stage.

### 1.6. Detailed Response

#### 1.6.1. Public Communication

- **Prepare Response Statements:** Develop clear, concise, and accurate statements for public release. Address the issue transparently, provide factual information, and outline steps being taken to resolve the situation.
- **Coordinate Messaging:** Ensure consistent messaging across all communication channels and avoid contradicting statements from different departments or team members.

#### 1.6.2. Technical Response

- **Investigate Incident:** Conduct a thorough investigation to determine the cause and impact of the threat. Document findings and response actions.
- **Mitigate Damage:** Implement technical solutions to address and resolve the issue, such as patching vulnerabilities, removing malware, or recovering compromised data.

## 1.7. Recovery and Resolution

### 1.7.1. Restore Normal Operations

- **Account Restoration:** Restore affected social media accounts to normal operation, ensuring that all security measures are in place and verified.
- **Content Review:** Review and clean up any compromised or harmful content from social media channels.

### 1.7.2. Post-Incident Actions

- **Impact Assessment:** Evaluate the impact of the threat on the organization, including damage to reputation, operational disruption, and any legal or regulatory implications.
- **Communication Follow-Up:** Provide updates to stakeholders and the public as necessary, and continue to address any remaining concerns or questions.

## 1.8. Post-Crisis Review

### 1.8.1. Incident Analysis

- **Debriefing:** Conduct a debriefing session with the Crisis Response Team to review the response actions, identify what worked well, and discuss areas for improvement.
- **Documentation:** Create a comprehensive report detailing the incident, response actions, and outcomes. Include lessons learned and recommendations for future preparedness.

### 1.8.2. Policy and Procedure Updates

- **Review and Update:** Review and update social media security policies, crisis response procedures, and training materials based on lessons learned from the incident.
- **Training and Drills:** Conduct regular training and simulation exercises for the Crisis Response Team and relevant employees to ensure preparedness for future incidents.

## 1.9. Ongoing Monitoring and Improvement

### 1.9.1. Monitor for Recurrence

- **Continuous Monitoring:** Maintain ongoing monitoring of social media channels to detect any signs of recurring threats or related issues.

- **Proactive Measures:** Implement proactive measures to strengthen social media security and prevent similar incidents in the future.

#### 1.9.2. Feedback and Improvement

- **Gather Feedback:** Collect feedback from the Crisis Response Team, employees, and stakeholders on the effectiveness of the response plan and areas for improvement.
- **Plan Updates:** Regularly review and update the crisis response plan to incorporate new threats, changes in social media platforms, and emerging best practices.

# 2. Social Media Account Dogpiling

---

## 2.1. Purpose

This strategy outlines the steps to be taken when an organization's social media account or a staff member's account is targeted by a dogpiling attack. **Dogpiling refers to a coordinated or spontaneous online harassment campaign where numerous users post negative, abusive, or harmful comments in a short period**. The purpose of this response strategy is to minimize harm, protect affected individuals, and manage the organization's reputation.

## 2.2. Scope

This strategy applies to all social media accounts managed by the organization, as well as personal accounts of employees.

## 2.3. Indicators of Dogpiling

Dogpiling doesn't always happen all at once. Often, there are early warning signs. If you notice any of the following, it's a good idea to stay alert and let your team know.

| What to look for | What it means |
|---|---|
| **Sudden flood of negative reactions** | A rapid increase in dislikes, angry emojis, or quote-tweets that seem designed to embarrass or shame, not just disagree. |
| **Huge spike in comments, mentions, or direct messages** | Your notifications suddenly blow up with a volume that is clearly out of the ordinary for your account. |
| **Fake-looking accounts** | Accounts with no profile picture, very few followers, or that were created recently. These are often used by people trying to hide who they really are. |

| | |
|---|---|
| **Inflammatory language, threats, or hate speech** | Comments include slurs, threats of violence, or language that attacks someone's identity (race, gender, sexuality, immigration status, etc.). |
| **Coordinated attacks using similar language** | Multiple accounts are posting the same or very similar messages, often using the same hashtags or phrases. |
| **Attacks spreading across platforms** | The same negative comments showing up on Facebook, Instagram, Tik Tok and even in your email all at once. This is a sign of a coordinated effort, not just one upset person. |
| **"Helpful" comments that feel off** | People who pretend to be supporters but leave comments that feel critical, condescending, or designed to make you doubt yourself. This is called "concern trolling." |

**Important:** Not every critical comment is a dogpile. People are allowed to question or disagree respectfully. If the volume is low and the language is civil, it may just be normal community feedback. Trust your instincts, if it feels like an attack, it probably is.

## 2.4. Immediate Response Steps

### 2.4.1. Employee Actions

Before doing anything else, take a moment. Close your eyes. Take three deep breaths. This attack is not your fault, and you are not alone. Your well-being matters more than any post or comment. When you feel ready, follow the steps below.

- **Do Not Engage:** Employees should avoid responding to or engaging with individuals participating in the dogpiling attack. Engaging can feed the attack and make it worse. Even if you feel defensive or want to correct misinformation, wait because responding in the moment often makes things worse.
- **Report Immediately:** Notify the social media team or designated incident response team as soon as the attack is detected. The sooner they know, the sooner they can help limit the damage.
- **Preserve Evidence:** Take screenshots and document the nature of the attack, including usernames, comments, and timestamps. Do this before attackers delete their posts or accounts. Do not respond to the attackers while doing this.
- **Ask for Backup:** If the attack feels overwhelming, ask a trusted colleague or friend to monitor your social media and report abusive content for you. This lets you step away and take a break while someone you trust has your back.
- **Protect Your Personal Information:** Review your privacy settings across all platforms. Make sure your personal phone number, home address, and private email are not publicly visible. This is especially important if the attack is spreading across multiple platforms.

### 2.4.2. Social Media Team/Incident Response Team Actions

- **Assess the Situation:**
  - **Content Review:** Review the content and scale of the dogpiling to assess its severity and potential impact on the organization or individuals.
  - **Source Identification:** Identify whether the attack is organic (spontaneous) or coordinated, and note any specific groups or accounts leading the attack.
- **Implement Defensive Measures:**
  - **Content Moderation:** Immediately moderate harmful content by hiding, deleting, or reporting comments and posts that violate platform policies.
  - **Adjust Account Settings:** Temporarily adjust account settings to limit further damage. This may include:
    - Restricting comments or who can reply
    - Turning off direct messaging
    - Enabling additional content moderation filters
    - Limiting quote posts to prevent your content from being used as a vehicle for harassment
    - "Detaching" or unlinking your original post from harmful quotes or replies if the platform allows
  - **Block and Report:** Block and report accounts that are primarily responsible for the attack, particularly those engaging in hate speech or threats.

## 2.5. Containment and Mitigation

### 2.5.1. Contain the Threat

- **Secure Social Media Accounts:** Ensure that all social media accounts are secure, with strong passwords and multi-factor authentication enabled. Consider temporarily limiting access to account managers only.
  - Decide if you want to temporarily turn off comments

### 2.5.2. Mitigate Impact on Individuals

- **Provide Support:**
  - **Emotional Support:** Dogpiling can trigger feelings of worthlessness, anxiety, depression, and even thoughts of self-harm. Offer counseling or support services to employees affected by the attack. Actively encourage affected staff to seek support from friends, family, or mental health professionals. Dealing with online attacks can be emotionally taxing, and no one should have to go through it alone.
  - **Temporary Social Media Break:** If the attack is particularly severe, consider temporarily taking down affected accounts or advising affected individuals to take a break from social media.

    - **Engage with Positive Communities:** Advise affected individuals to intentionally spend time in positive online spaces or with close contacts who uplift them. This helps counter the negativity of the attack.
    - **Remove targeted individuals from sensitive communications** until situation settles
- **Public Communication:**
    - **Statement of Response:** Prepare a carefully worded public statement if necessary, acknowledging the situation, condemning harassment, and emphasizing the organization's values. Avoid escalating the situation or engaging directly with attackers.
    - **Monitor Public Sentiment:** Continuously monitor public sentiment and media coverage to adapt the response strategy as needed.

## 2.6. Recovery and Communication

### 2.6.1. Account Recovery

- **Restore Normal Operations:** Once the attack subsides, gradually restore normal account settings and continue to monitor for any resurgence of the attack.
- **Content Review:** Review all content and communication during the attack to ensure that no harmful posts remain visible and that all inappropriate comments have been addressed.

### 2.6.2. Internal Communication

- **Brief Employees:** Provide a briefing to employees, especially those involved in managing social media accounts, on the incident and the steps taken. Offer guidance on handling similar incidents in the future.

### 2.6.3. External Communication

- **Proactive Engagement:** If consensus is reached internally then consider engaging with followers and the community to reaffirm the organization's commitment to its values and to support positive online interaction.
- **Stakeholder Communication:** If the incident has broader implications, communicate with key external stakeholders, such as partners or clients, to reassure them of the organization's stability and approach to managing online threats.
- **Flood the Space with Positivity:** If the attack used a specific hashtag or comment thread, consider asking your supportive community to share positive messages using that same hashtag. This helps drown out the negativity and reminds everyone of the good work you do.

ODLAN

# 3. Social Media Account Cloning (Instagram)

## 3.1. Purpose

This strategy outlines the steps to be taken when an organization's Instagram account or a staff member's personal Instagram account is cloned (aka impersonation or account spoofing). **Account cloning occurs when someone creates a fake account using your name(s), photos, or bio to deceive your followers, staff, or community members**. The attacker may use the cloned account to ask for money, additional personal information, password and login information or redirect unsuspecting people to spam and scam websites or links.

## 3.2. Scope

This strategy applies to the organization's official Instagram account(s) and personal Instagram accounts of employees. The scope of this includes any social media platforms where cloning may occur.

## 3.3. Indicators of Account Cloning

Account cloning can happen quickly. Sometimes you'll notice it yourself, but often your community members will alert you. If you notice any of the following, it's a good idea to stay alert and let your team know.

| What to look for | What it means |
|---|---|
| **A fake account using your profile photo, name, or bio** | Followers, clients, or partners message you asking, "Did you make a new account?" or "Is this your new page?" |
| **Your community members asking if you created a new account** | Someone has copied your profile picture, username (or a slight variation), and bio to create a lookalike account. |
| **The fake account is messaging your followers** | Your community members report receiving direct messages from the fake account asking for money, personal information, or clicks on suspicious links. |
| **The fake account is reposting your content** | The cloned account is copying your posts, stories, or highlights to appear legitimate. |
| **The fake account is** | You notice a new account (often private) following many of your |

| | |
|---|---|
| **following your followers** | followers in a short period. |
| **The fake account blocked your real account** | The impersonator has blocked you to stay hidden so you can't find the account when searching from your profile. |
| **A sudden drop in engagement or trust** | Followers seem hesitant to engage with your real account, or you receive messages asking, "Are you legit?" |

## 3.4. Immediate Response Steps

### 3.4.1. Employee Actions

- **Do Not Engage:** Employees should avoid responding to or engaging with individuals participating in the dogpiling attack. Engaging can feed the attack and make it worse. Even if you feel defensive or want to correct misinformation, wait because responding in the moment often makes things worse.
- **Report Immediately:** Notify the social media team or designated incident response team as soon as the attack is detected. The sooner they know, the sooner they can help limit the damage.
- **Change Your Profile Picture:** Update your profile picture to help your community distinguish your real account from the clone. This visual change makes it easy for followers to tell at a glance which account is real.
- **Warn Your Community (If Safe to Do So):** If the fake account is actively messaging your followers (especially asking for money or personal information), post a quick warning on your real account. Keep it simple and calm.
    - Example: "We've been made aware of a fake account pretending to be us. Please do not engage with or send money to any account other than our official one. We are working to resolve this."
- **Preserve Evidence:** Take screenshots and document the nature of the attack, including usernames, comments, and timestamps. Do this before attackers delete their posts or accounts. Do not respond to the attackers while doing this.

### 3.4.2. Social Media Team/Incident Response Team Actions

- **Implement Defensive Measures:**
    - **Report to Instagram:** The account holder (or the person being impersonated) should file the official impersonation report with the platform. This is the most effective route . The team should also ask several trusted contacts to report the counterfeit profile under "Pretending to be someone" or "Fake profile," as multiple reports can speed up the platform's review
    - **Alert Your Community**: Post a clear, calm warning on your official account. Include:

        - Confirmation that the fake account is not affiliated with you
        - A request for followers to report the fake account
        - Clear instructions on how to identify your real account (e.g., "We only have one account. We will never ask for money via DM.")
        - A warning to not accept any new or duplicate friend/follow requests that seem to come from your account
    - **Secure Your Official Account (see 3.5.1 for more detail):** Immediately change your password and enable two-factor authentication (2FA) if it's not already active
    - **Monitor for Additional Clones**: Impersonators sometimes create multiple accounts. Keep monitoring for new fake accounts.

## 3.5. Containment and Mitigation

### 3.5.1. Secure Your Official Account

- **Immediate Security Actions:**
    - **Change your password** to a strong, unique password .
    - **Enable multi-factor authentication (2FA)** if you haven't already .
    - **Review login sessions** and log out of any unfamiliar devices.
    - **Review third-party apps** connected to your Instagram account and remove any you don't recognize.
    - **Consider changing your username slightly** if the impersonator has created a very similar username that could confuse followers.
    - **Temporarily limit account access** to only essential team members until the situation is resolved.

### 3.5.2. Mitigate Impact on Individuals

- **Support Your Community:**
    - **Acknowledge and Validate:** If any community members were scammed or harmed by the fake account, acknowledge their experience and offer support or guidance on next steps (e.g., contacting their bank, reporting to authorities).
    - **Provide Clear Guidance:** Clearly explain how followers can identify your real account and how they can protect themselves from similar scams in the future.
    - **Be Transparent**: If the clone posted harmful content, address it honestly and directly. Reaffirm your organization's values.
- **Support Affected Staff:**
    - **Emotional Support**: Being impersonated online can feel violating and unsettling. Offer counseling or support services to employees affected by the clone. Encourage staff to seek support from friends, family, or mental health professionals.
    - **Temporary Break**: If the situation is particularly stressful, advise affected individuals to take a break from social media.

- **Engage with Positive Communities**: Encourage affected staff to spend time in positive online spaces or with close contacts who uplift them.
- **Remove targeted individuals from sensitive communications** until the situation settles.

## 3.6. Recovery and Communication

### 3.6.1. Account Recovery

- **After the Fake Account is Removed:**
  - **Confirm Removal:** Once Instagram removes the fake account, confirm this with your team and your community.
  - **Restore Normal Operations:** Gradually restore normal account settings and continue to monitor for any resurgence of the attack.
  - **Content Review:** Review all content and communication during the attack to ensure that no harmful posts remain visible and that all inappropriate comments have been addressed.
  - **Post-Event Security Review:** Conduct a brief review of what happened, how it was handled, and what could be improved.

### 3.6.2. Communications

- Brief affected employees on the incident and reinforce security best practices for future situations. If the incident has broader implications, reassure key stakeholders and address community concerns transparently.

ODLAN

# 4. Social Media Account Hacked

## 4.1. Purpose

This strategy outlines the steps to be taken when an organization's social media account or a staff member's account is hacked. **A hack occurs when an unauthorized person gains access to an account, often to steal information, send spam, scam contacts, or damage reputation.** The goal is to regain control quickly, minimize harm to the organization and affected individuals, and prevent future incidents.

## 4.2. Scope

This strategy applies to all social media accounts managed by the organization, as well as personal accounts of employees.

## 4.3. Indicators of a Hacked Account

A hack can be obvious (you are locked out) or subtle. Recognizing these red flags early is critical for minimizing damage.

| What to look for | What it means |
|---|---|
| **You are locked out or can't log in** | Your password has been changed, or the hacker has changed the recovery email or phone number associated with the account. |
| **Unexpected password reset or recovery emails** | You receive emails from the platform about password changes or recovery requests you didn't initiate. |
| **Login alerts from unfamiliar locations** | You receive notifications about logins from devices, cities, or countries you have never used. |
| **Unusual changes to your account, posts, stories, or messages** | You notice your profile photo, name, bio, email address, or phone number has been changed without your knowledge. You see content you didn't create, such as spammy links, offensive material, or direct messages to your contacts asking for money or personal information. |
| **Friends or followers report suspicious activity** | Your contacts tell you they received strange messages or posts from your account. |

## 4.4. Immediate Response Steps

#### 4.4.1. Employee Actions

- **Do Not Engage:** If the hacker is messaging you or posting from your account, do not reply or engage with them. Engaging can alert them that you are active and may cause them to escalate their actions.
- **Check if You Can Still Log In:**
    - **If YES:** Change your password immediately to a strong, unique one. Do not use a password you have used anywhere else.
    - **If NO:** You have been locked out. Go directly to the platform's login page and use the "Forgot Password?", "Need Help?", or "My account was hacked" link to start the official account recovery process.
- **Report Immediately:** Notify your organization's social media team or designated incident response team. They can provide support and help coordinate further action.
- **Preserve Evidence:** Take screenshots and document the nature of the attack, including unauthorized posts, messages, and login alerts, any changes to your profile information, any threatening or suspicious messages you received.
- **Warn Your Community (If You Can):** If you have access to another account (or can post from a friend's account), post a brief warning to your followers.
    - For example: *"Our [Platform] account @[username] was hacked. Please ignore any recent messages or posts. Do not click any links or send money. We are working to resolve this."* This protects your network from being scammed.

#### 4.4.2. Social Media Team/Incident Response Team Actions

- **Assess the Situation:**
    - **Account Identification:** Identify the compromised account(s) and the scale of the breach.
    - **Impact Assessment:** Determine what the hacker has done (e.g., posted spam, messaged contacts, changed settings).
    - **Coordinate with Employee:** If an employee's account was hacked, work with the affected employee to support their recovery attempts and provide guidance.
- **Provide Support and Escalate:**
    - **Assist with Recovery (Employee Account Hacked):** If the employee is having trouble recovering the account, help them navigate the platform's official recovery process, which may involve verifying their identity with a photo ID or answering questions about their account history .
    - **Secure Linked Systems:** If the hacked account was a business account, ensure advertising accounts, business managers, and social media management tools are also secured and that admin permissions are revoked.
    - **Check for Secondary Access:** Once access is regained, review active sessions, connected apps, and recovery settings to ensure the hacker has left no "back doors".

## 4.5. Containment and Mitigation

#### 4.5.1. Secure the Account and Related Systems

- **After Regaining Access, Immediately:**
    - **Force Logout of All Devices:** Use the platform's security settings to sign out of all active sessions, kicking the hacker out .
    - **Enable Two-Factor Authentication (2FA):** Turn on 2FA immediately using an authenticator app (e.g., Google Authenticator, Microsoft Authenticator) rather than SMS text messages, which are less secure. Save any backup codes provided in a safe, offline location .
- **Verify and Update Recovery Options:** Review and remove any unfamiliar email addresses, phone numbers, or backup codes. Ensure all recovery information is correct and belongs to you .
- **Remove Unfamiliar Connections:** Revoke access for any third-party apps or integrations you do not recognize or no longer use .
- **Scan Your Devices:** Run a full security scan on the device you use to access social media to check for malware that might have captured your password. Perform this scan before changing passwords again. Some scanning tools include:
    - Microsoft Defender Antivirus (built into Windows): https://support.microsoft.com/en-us/defender/getting-started-with-microsoft-defender
    - Bitdefender: https://www.bitdefender.com/en-us/consumer/free-antivirus
    - Malwarebytes: https://www.malwarebytes.com/solutions/virus-scanner

#### 4.5.2. Mitigate Impact on Individuals and the Organization

- **Support the Affected Employee:**
    - **Emotional Support:** Being hacked can feel like a violation. Offer counseling or support services to the employee. Encourage them to seek support from friends, family, or professionals.
    - **Temporary Break:** If the incident is especially stressful, advise the employee to take a temporary break from social media management duties.
    - **Remove from Sensitive Communications:** Temporarily remove the affected individual from sensitive internal communications until the account is fully secured.
- **Support Your Community:**
    - **Acknowledge and Validate:** If any community members were scammed or harmed by the hacker's activity, acknowledge their experience and offer clear guidance on what to do next (e.g., change their passwords, be wary of suspicious links).

    - **Be Transparent:** Post an honest and clear update about the situation. Explain what happened, what you have done to fix it, and how you are preventing it from happening again. This helps rebuild trust .
    - **Warn About Phishing:** Remind your community to be cautious of suspicious links and to verify requests for personal or financial information.
- **Report the Incident:**
    - **To the Platform:** Use the platform's official channels to report the compromise. This helps them investigate and potentially take action against malicious actors.

## 4.6. Recovery and Communication

### 4.6.1. Account Recovery

- **Restore Normal Operations:** Once the account is secured, gradually resume normal posting and activity. Confirm that all recovery methods (email, phone, 2FA) are functioning correctly.
- **Content Review:** Review and clean up any unauthorized content posted during the hack to ensure that no harmful posts remain visible.

### 4.6.2. Internal Communication

- **Brief Employees:** Provide a briefing to staff about the incident, the steps taken, and the outcome. Use the incident as a training opportunity. Reiterate best practices for security:

### 4.6.3. External Communication

- **Rebuild Trust and Reclaim Your Message:**
    - Once the account is secure, post a final update to your community confirming the issue is resolved and thanking them for their understanding.
    - Reaffirm your organization's values and commitment to protecting your community's safety.
    - If a positive relationship with your audience was damaged, consider hosting a Q&A or sharing behind-the-scenes content to reconnect and model authenticity.
- **Document Everything:** Compile a report of the incident, including timelines, actions taken, and lessons learned, to improve future responses and security posture.

ODLAN

# 5. Website Attack

## 5.1. Purpose

This strategy outlines the steps to be taken when an organization's website is attacked or compromised. The objective is to minimize damage, restore normal operations, and prevent future incidents.

## 5.2. Scope

This strategy applies to all websites owned or operated by the organization, including associated web applications, databases, and servers. It covers a range of potential attacks, including but not limited to Distributed Denial of Service (DDoS) attacks, website defacement, malware injection, SQL injection, and unauthorized access.

## 5.3. Indicators of a Website Attack

Website attacks don't always announce themselves loudly. Sometimes the signs are subtle. If you notice any of the following, it's important to stay alert and notify your team right away.

| What to look for | What it means |
|---|---|
| **Unusual spikes in traffic** | A sudden, massive increase in visitors, especially from unknown sources, unusual geolocations, or a wide range of IP addresses that don't match normal patterns. This could be an attack designed to overwhelm and crash your site. |
| **Slow website performance or downtime** | Your website loads very slowly, times out, or becomes completely unavailable. This is often a direct result of the traffic spike above. |
| **Website defacement** | Unauthorized changes to your website's content, images, layout, or code. The site may look different, display strange messages, or have new, unfamiliar pages. |
| **Unauthorized redirects to other websites** | Visitors are automatically sent to a different website without their consent. This is often used to send users to scam or phishing sites. |
| **Malware or malicious scripts** | Security scans or monitoring tools detect harmful code, files, or scripts on your website. These may have been planted to steal data, spread viruses, or give attackers ongoing access. |

| | |
|---|---|
| **Alerts from security tools** | Your security tools (firewalls, intrusion detection systems, logging systems) flag suspicious activity such as:<br>- **Multiple failed login attempts** (especially from the same IP or many different IPs)<br>- **Unauthorized access** (unrecognized users or devices logged in). This means an attacker may have gained access.<br>- **Changes to files** (files modified, added, or deleted without your knowledge). This could indicate an attacker is planting malicious code, stealing data, or covering their tracks.<br>- **Unusual data leaving your system** (large amounts of information being sent out). This could mean data is being stolen |

**Important**: Not every slow-loading page or error message means you've been hacked. Sometimes the cause is a technical glitch, server issue, or routine maintenance. However, if you notice a combination of these indicators, especially unusual traffic paired with performance issues or alerts, treat it as a potential attack and activate your incident response plan.

## 5.4. Immediate Response Steps

### 5.4.1. Employee/Administrator Actions

- **Report Immediately:** If you suspect that the website is under attack, report the incident to the IT department or the designated website security team immediately.
- **Do Not Modify:** Avoid making any changes to the website until the security team has been notified and has taken control of the situation.
- **Collect Information:** Document any suspicious activities, including screenshots, error messages, and any relevant logs.

### 5.4.2. IT Department/Website Security Team Actions

- **Isolate the Threat:**
    - **Take the Website Offline:** If necessary, take the website offline temporarily to prevent further damage or data loss.
    - **Restrict Access:** Limit access to the website and associated systems to essential personnel only.
    - **Identify the Attack:** Use monitoring tools and logs to identify the type of attack and the entry point used by the attackers. Some monitoring tools include:
        - Google Analytics: https://analytics.google.com/analytics/web/provision/#/provision
        - Query Monitor: https://wordpress.org/plugins/query-monitor/
        - Galileo: https://www.cloudflare.com/en-ca/galileo/
    - **Implement a Status Page.** Fail over to a status page (e.g., status.yourorg.org) to inform users the service is down and buy time to fix the issue. This is an alternative to simply taking the site offline.

- **Communicate Internally:**
  - Inform relevant stakeholders, including executive leadership, the communications team, and legal counsel, about the incident and initial steps taken.
  - Coordinate with the public relations team to prepare for potential external communication if the incident is severe.
- **Apply Temporary Fixes:** Implement temporary measures, such as blocking malicious IP addresses, disabling vulnerable features, or applying patches to prevent the attack from spreading or escalating.
- **Regional Blocking/Geofence**:
  - Implement geographic access controls to block or restrict traffic originating from specific countries or regions. This is a temporary measure to mitigate attacks that appear to originate from certain geographic areas.
  - **How it works:** Regional blocking relies primarily on the IP address of incoming requests. The server checks the IP against geolocation databases to determine the country of origin.
  - **When to use:**
    - To block traffic from regions known to be sources of attacks or with high cybercrime activity
    - To restrict access to services that are only available in certain countries
    - As an additional layer of defense during an ongoing attack
  - **Implementation:**
    - Configure your Web Application Firewall (WAF) or DDoS protection service to block or rate-limit traffic from specific regions
    - Consider using a combination of IP blocking, rate limiting, and other measures for more effective defense

## 5.6. Recovery and Communication

### 5.6.1. System Recovery

- **Restore Services:** Once the website is secure, restore it to normal operation, using clean backups if necessary.
- **Monitor for Further Activity:** Monitor the website closely for any signs of continued malicious activity, unauthorized access attempts, or other anomalies.
- **Patch Vulnerabilities:** Identify and patch any vulnerabilities that were exploited, such as outdated software, insecure configurations, or weak passwords.
- **Reset Credentials:** Reset all credentials associated with the website, including administrative passwords, database passwords, and API keys, and enforce stronger password policies.
- **Traffic Filtering:** Implement rules to block traffic from suspicious IP ranges or countries if the attack is geographically concentrated.

### 5.6.2. Internal Communication

- **Debrief Teams:** Provide a detailed debrief to all relevant teams, including IT, communications, and leadership, about the incident and the steps taken to secure the website. Frame the investigation as looking for failures in processes rather than scapegoats.
- **Review Access Controls:** Review and update access controls, ensuring that only authorized personnel have the necessary permissions.

#### 5.6.3. External Communication

- **Inform Users:** If user data was compromised or the attack had a significant impact, inform affected users promptly and provide guidance on any actions they should take (e.g., changing passwords).
- **Public Statement:** Prepare and release a public statement, if necessary, acknowledging the incident and explaining the steps taken to resolve it and prevent future occurrences.
- **Notify Authorities:** If the attack involved data breaches or illegal activities, notify the relevant law enforcement agencies or regulatory bodies.

## 5.7. Proactive Backup Strategy

Regular, automated backups are essential for recovering from a website attack, whether it's a defacement, malware infection, or data loss incident. These backups will help restore the website quickly in the event of an attack, defacement, or data loss.

- **What to Back Up:**
  - All website files (HTML, PHP, images, etc.)
  - Databases (e.g., user data, content, configurations)
  - Configuration files (e.g., server settings)
  - SSL certificates and keys
  - Any custom scripts or applications
- **How:**
  - **Daily full backups** (or more frequently for high-traffic sites) on an automated schedule
- **Where to Store:**
  - **Multiple locations**: Keep backups in at least two separate, secure locations (such as one on external server and one in the cloud)
  - **Versioned**: Retain multiple versions (e.g., last 7 daily backups, last 4 weekly backups, last 12 monthly backups) to restore from a point before the attack occurred
- **Test Your Backups:**
  - **Test restores regularly** (at least monthly) to ensure your backups are valid and your restoration process works
  - **Document the restoration process** and assign responsibility to specific team members
  - **Time your restores** so you know how long it will take in a real emergency

- **Using the Internet Archive:**
  - The Wayback Machine (archive.org) can help recover **public-facing content** if backups are unavailable
  - It is **not a substitute for your own backups**. This only captures publicly visible pages and may not capture dynamic content, databases, or private data
- **Retention and Disposal:**
  - Establish a retention policy based on your organization's needs and compliance requirements
  - Securely dispose of old backups when they are no longer needed to prevent data exposure

ODLAN

# 6. Email Phishing

## 6.1. Purpose

This strategy outlines the steps to be taken when an email phishing attempt is detected or suspected within the organization. The goal is to minimize the impact, prevent data breaches, and enhance the organization's overall cybersecurity posture.

## 6.2. Scope

This strategy applies to all employees, contractors, and third-party vendors who have access to the organization's email systems and for individuals personal emails. It covers all forms of phishing, including spear-phishing, whaling, and generic phishing attacks.

## 6.3. Indicators of Phishing

Spotting these red flags early is critical for preventing data breaches and reducing harm.

| What to look for | What it means |
|---|---|
| **Unexpected emails from unknown or suspicious senders, especially those requesting sensitive information.** | Someone is impersonating a trusted organization or individual to trick you into sharing sensitive information. |
| **Emails containing suspicious links or attachments.** | The link leads to a fake login page designed to steal your credentials, or the attachment contains malware that can infect your device. |
| **Unsolicited/Urgent requests for login credentials, personal/financial information or gift cards.** | The sender is creating false urgency to pressure you into acting quickly without thinking to steal your credentials or money. |
| **Messages that appear to be from senior leadership but are from an unfamiliar email address/phone number.** | Someone is impersonating a leader to manipulate you into sending money, gift cards, or sensitive data. |

## 6.4. Immediate Response Steps

### 6.4.1. Employee Actions

- **Do Not Engage:** Do not click on any links, open any attachments, or reply to the suspicious email.
- **Check Authenticity**: If you are unsure/suspicious, use a secondary communication channel to verify. For example, if the first contact was via email then verify through Slack.

- **Report Immediately:** Do not forward the phishing email. Send screenshots to the organizational team with the subject line "Suspected Phishing". If using Microsoft Outlook or Gmail, you can use the built-in reporting button.
- **Isolate the Threat:** If a phishing link or attachment has been clicked, disconnect the device from the network immediately and inform the team.

#### 6.4.2. Social Media Team Actions

- **Analyze the Email:** Investigate the reported email to determine if it is indeed a phishing attempt. Use tools to analyze links, attachments, and sender information.
- **Block and Quarantine:** Block the sender and quarantine the email across the organization's email systems to prevent further exposure.
- **Scan Affected Systems:** If the phishing email was interacted with, conduct a full malware and virus scan on the affected device(s).
- **Change Credentials:** If login credentials were compromised, immediately instruct the employee to change their passwords. Consider enforcing a system-wide password reset if necessary.

ODLAN

# 7. Doxxing (Personal Information Leaked)

## 7.1. Purpose

This strategy outlines the response plan for when a member of the organization has their **personal information leaked online, also known as doxxing**. Doxxing is the malicious publication of private information such as home addresses, phone numbers, or family details, without consent, often to intimidate, harass, or out an individual's identity. The objective is to protect the individual's safety, mitigate potential damage to the organization, and manage the situation effectively.

## 7.2. Scope

This strategy applies to incidents involving the unauthorized disclosure of personal information of any member of the organization's team. This includes information such as home addresses, phone numbers, email addresses, family details, sexual orientation, gender identity and other sensitive personal data.

## 7.3. Indicators of Doxxing

Recognizing these signs early is critical for protecting the affected individual's safety and responding quickly.

| What to look for | What it means |
|---|---|
| **Personal information posted on social media, forums, or other websites** | The individual's private details such as home address, phone number, email, or family details have been published without consent. |
| **Threatening or harassing communications directed at the team member or their family members.** | Someone is using the exposed information to intimidate, threaten, or harass the individual or their family members. |
| **Sudden increase in unwanted contacts** | Receiving a spike in calls, emails, messages, or unexpected visitors at their home. This often means their contact information has been widely shared and others are acting on it. |
| **Reports from colleagues, media, or law enforcement about exposed information** | Others have discovered the individual's personal information online and are alerting them. |

### 7.3.1. Early Warning System

- Set up Google Alerts for leadership members, executives, and official organizational accounts (including social media handles) to monitor potential doxxing threats. General members can set up alerts for their own individual accounts separately.
- Use a data breach service to monitor if your email has been part of a data breach. Such as HaveIBeenPwned: https://haveibeenpwned.com/

## 7.4. Immediate Response Steps

### 7.4.1. Team Member's Actions

- **Report Immediately:** The affected team member should immediately report the doxxing incident to the organization's leadership team or designated point of contact.
- **Limit Exposure:** Refrain from engaging with or responding to any communications or threats received as a result of the doxxing.
- **Document the Incident:** Keep records of all instances of harassment, including screenshots, emails, messages, and any other relevant evidence.

### 7.4.2. Crisis Response Team Actions

- **Verify the Incident:**
  - **Assess the Information:** Verify the accuracy and scope of the leaked information and determine where it was posted.
- **Information Security Measures:**
  - Assist the individual in securing their personal digital accounts, including changing passwords, enabling multi-factor authentication, and reviewing account activity.
    - Review the Social Media Security & Privacy Handbook on ODLAN's website for applicable privacy settings
- **Mitigate Online Exposure:**
  - **Request Removal:** Contact website administrators, social media platforms, and search engines to request the removal of the leaked information.
  - **Legal Action:** Explore legal options, such as cease and desist orders, to compel the removal of personal information and to prevent further dissemination. Consider the following legal options:
    - LEAF https://www.leaf.ca/
      - The Women's Legal Education and Action Fund (LEAF) is a national charitable organization that advances gender equality through law.
    - QMUNITY https://www.qmunity.ca/legal-clinic
      - QMUNITY has been a resource centre providing essential programs and services to 2SLGBTQIA+ individuals and allies in BC, Canada.
    - Call/Acal https://prismeconference.ca/

- The Canadian Association of LGBTQ2S+ Lawyers is a national association of 2SLGBTQ+ legal professionals dedicated to developing an inclusive, innovative and representative bar, in every jurisdiction across Canada.

- **Decide when necessary to notify Law Enforcement:** Contact local law enforcement to report the doxxing incident and seek their assistance if there is a threat to the individual's safety.

## 7.5. Support for the Affected Individual

- **Emotional Support:** Provide access to counseling services or support resources for the affected team member and their family members to help manage the emotional impact of the doxxing.
- **Ongoing Monitoring:** Continue monitoring online platforms for further leaks or threats, and keep the individual informed of any developments.

# 8. Self-Care Recommendations for After Being Doxxed

---

Being doxxed (having personal information exposed publicly without consent) can be a distressing experience. It's important to prioritize self-care and take steps to address both emotional and practical concerns. Here are some self-care recommendations for managing the aftermath of being doxxed:

## 8.1. Emotional Self-Care

### 8.1.1. Acknowledge Your Feelings

- **Validate Your Emotions:** It's normal to feel a range of emotions, including anger, fear, or anxiety. Allow yourself to feel and express these emotions without judgment.
- **Seek Support:** Talk to trusted friends, family members, or a mental health professional about your experience. Sharing your feelings can help alleviate some of the emotional burden.

### 8.1.2. Practice Stress-Reduction Techniques

- **Mindfulness and Relaxation:** Engage in mindfulness practices, such as meditation or deep-breathing exercises, to help manage stress and anxiety.
- **Physical Activity:** Regular exercise can help reduce stress and improve overall well-being. Activities like walking, yoga, or other forms of exercise can be beneficial.

### 8.1.3. Establish Boundaries

- **Limit Exposure:** If the doxxing incident has resulted in negative online interactions, consider taking a break from social media or limiting your exposure to distressing content.
- **Create Safe Spaces:** Engage in activities and spend time in environments that make you feel safe and supported.

## 8.2. Practical Self-Care

### 8.2.1. Build a Support Network

- **Seek Community Support:** Connect with support groups or organizations that specialize in online harassment or doxxing. They can offer guidance, resources, and a sense of community.

- **Maintain Relationships:** Stay connected with friends and family who can provide emotional support and practical assistance during this time.
- **Inform Friends and Family:** Let your trusted contacts know about the situation, as doxxers may target them too. Encourage them to tighten their own privacy settings

#### 8.2.2. Engage in Positive Activities

- **Pursue Hobbies:** Engage in activities that bring you joy and fulfillment. Hobbies and interests can provide a healthy distraction and improve your overall mood.
- **Focus on Self-Care:** Prioritize activities that contribute to your well-being, such as getting adequate rest, maintaining a healthy diet, and engaging in activities that promote relaxation and happiness.

#### 8.2.3. Proactive Measure: Dox Yourself

One of the most effective ways to protect yourself from doxxing is to see what information about you is already publicly available and remove it before someone else can use it against you .

- **Search Yourself Online:** Use different search engines (Google, DuckDuckGo, etc.) to search for: your full name, usernames, email addresses, phone numbers, home address
- **Audit Your Social Media Profiles:** Review every social media account you have (Facebook, Instagram, LinkedIn etc.). Check what information is visible to the public. Use an incognito/private browser window to view your profile as a stranger would. Remove or hide any personal details
- **Review Connected Accounts and Old Profiles:** Delete or deactivate old accounts you no longer use (e.g., Wattpad, Tumblr, old forums, etc.). Check which third-party apps have access to your social media accounts and remove any you don't recognize or no longer use.

### 8.3. Professional Help

#### 8.3.1. Seek Therapy or Counseling

- **Mental Health Support:** Consider working with a therapist or counselor who can help you process the trauma and develop coping strategies. They can provide a safe space to explore your feelings and work through the impact of the incident.

#### 8.3.2. Legal Consultation

- **Legal Advice:** If you are facing ongoing harassment or have concerns about legal implications, consult with a legal professional who specializes in privacy or cyber law.

---

**Important Note:** Each individual's experience with doxxing is unique, and self-care needs may vary. It's essential to tailor these recommendations to your specific situation and seek

professional advice if needed. By taking these steps, you can better manage the emotional and practical challenges following a doxxing incident, and work towards reclaiming a sense of safety and well-being.

# References


Akomea, C. B. (2025, June 11). *Incident response for ddos attacks and the way forward*. Cyber Security Cue. https://cybersecuritycue.com/incident-response-for-ddos-attacks/

Cyberhaven. (2026, February 12). *What is a ddos attack?*. https://www.cyberhaven.com/infosec-essentials/ddos-attack

Dach, P. (2025, September 7). *Dogpiling (internet) and online harassment*. Go2Share. https://www.go2share.net/article/dogpiling-internet

Ferriss, T. (2026, June 23). *How to stop dogpiling on social media?*. SkyJob Net.Com. https://skyjobnet.com/how-to-stop-dogpiling-on-social-media.html

Gonzalez, C. (2023, May). *Coalition against online violence | Mapping report 2024.* International Women's Media Network. https://onlineviolenceresponsehub.org/wp-content/uploads/2024/01/CAOV-MAPPING-REPORT-2024.pdf

Johnson, K. (2025, March 11). *Incident response for web application attacks*. Tech Target. https://www.techtarget.com/searchSecurity/feature/Incident-response-for-web-application-attacks

Knutsson, K. (2026, January 9). *Cloned on Facebook? Here's how to take back control*. CyberGuy. https://cyberguy.com/security/cloned-on-facebook-heres-how-to-take-back-control/

ODLAN. (2025). *Digital safety procedural policy.* https://odlan.ca/digital-safety-procedural-policy/

PrivacyOn. (2026, April 30). *Privacy guide for LGBTQ+ individuals: Protecting your identity online.* https://www.privacyon.com/blog/privacy-guide-for-lgbtq-individuals

Terassa, D. (2026, January 31). *How to detect if a website is blocking you by region.* Technobits. https://tecnobits.com/en/Web-blocking-by-region/

TSPA. (2023, July 31). *Responding to and preventing doxing: A TSPA resource.* https://www.tspa.org/wp-content/uploads/2023/07/Responding-to-and-Preventing-Doxing_-A-Resource-For-the-public.pdf