Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
Camp BGen Rafael T Crame, Quezon City

MEMORANDUM

FOR : See Distribution

FROM : D, ITMS

SUBJECT : **Cyber Security Advisory: Information Manipulation and Disorder**

DATE : September 16, 2022

---

1. Reference: Announcement from Cybersecurity and Infrastructure Security Agency (CISA) MIS, DIS, MAL-INFORMATION (MDM).

2. The above reference is to the Cybersecurity and Infrastructure Security Agency's (CISA) safety measures to prevent the spread of information disorder namely: Misinformation, Disinformation, and Mal-information (MDM).

3. Information manipulation is done to weaken public opinion, trust, and information validity. This encompasses the use of both new (content service platforms) and classic (print) media to sow discord, divide trust, and spread confusion in communities.

4. Malicious actors utilize MDM to disrupt and destroy national cohesion, causing chaos, confusion, and conflict. Using organized illegal cyber attacks, such as account hijacking and defacing public-facing websites, to influence and divide public opinion and trust. The types of information disorders are described as follows:

a. Misinformation is false, but not created or shared with the intention of causing harm;

b. Disinformation is false information that is deliberately created to mislead, harm, or manipulate a person, social group, organization, community, or country; and

c. Mal-information, is information that is based on fact but used out of context to mislead a person, social group, organization, community, or country.

5. Malicious actors employ a number of tactics to persuade victims, compel them to behave, and cause confusion. The following are the tools used to distribute MDM:

a. Manipulated audio/video, audio/video content that captures the public's attention and is repeatedly disseminated. This manipulated content is dangerously effective at spreading false information;
b. Cheap fakes are real audio and video clips that have been sped up, slowed down, or shown out of context to mislead;
c. Deepfakes are fake but very convincing audio and video clips that have been crafted and spread to deceive. It can persuade you that people said or did things that did not happen. It can generate plausible-looking phony faces or full-body films. An audio deepfake is a voice clone that generates new phrases from one or more persons on its own or in conjunction with a fake video;
d. Forged artifacts, a common feature that employs forged letterheads, copied and pasted signatures, made-up social media postings, and maliciously edited emails. Such forgeries are created and spread for a variety of malicious motives. To increase their credibility, forgeries are frequently presented as the result of a hack, theft, or other interception of documents—they claim to be "leaked" materials; and
e. Proxy websites are fronts for malicious actors, designed to launder disinformation and divisive content or to drive website visits. These websites are not designed to deliver accurate information. Following high-profile events, these websites will spring up to capitalize on the public's real need for knowledge. Be wary of sites with unknown origins. Both the information and its sources must be reliable.

6. Hereunder are the techniques for increasing readiness and promoting resilience against MDM:

a. Confirm its veracity with numerous sources;
b. Remain vigilant. Forgeries can be disguised as legitimate content to give them legitimacy. If the forgery appears to be breaking news, check reputable news sites to see if they are covering the event;
c. A misspelled URL may indicate that a website is not a reliable source;
d. Use multiple fact-checking tools to verify the authenticity and trustworthiness of information;
e. Rely on trusted sources such as national and local authority websites and verified authorized social media accounts. Rely on national and local health officials for health and safety updates;
f. Be prepared, participate, get involved, and be knowledgeable about current events in national and local communities;
g. Think twice before sharing content online;
h. Be cautious when posting Personal Identifiable Information (PII). Personal identification, images, or other information may be used to spread MDM;
i. Be wary of content that appears manipulative or too emotive. Be especially cautious of information that seeks to incite rage or division; and,
j. Report the incident to the National Computer Emergency Response Team (NCERT-PH), the National Bureau of Investigation, or the Philippine National Police, Anti-Cyber Crime Group (PNP-ACG).

7. In view of the foregoing, this Service recommends the uploading of the attached info-graphic material on your respective websites and social media platforms to promote information security awareness to PNP personnel and to the community.

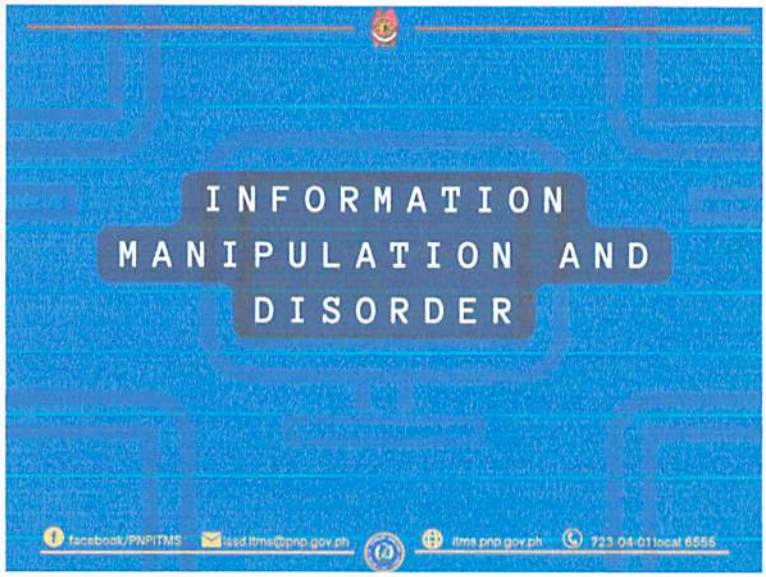
8. You may visit itms.pnp.gov.ph to download learning materials regarding cybersecurity under the Computer Security Tab. Should you have any inquires or concerns, you may contact ISSD at 8723-0401 local 6546 or e-mail us at issd.itms@pnp.gov.ph.

9. For widest dissemination.

HARRIS R FAMA
Police Brigadier General

Distribution:
IG, IAS
Cmdr, APCs
D-Staff
P-Staff
D, NSUs
RD, PROs

Copy Furnished:
Command Group
SPA to the SILG



INFORMATION MANIPULATION

Information manipulation is done to weaken public opinion, trust, and information validity. This encompasses the use of both new (content service platforms) and classic (print) media to sow discord, divide trust, and spread confusion in communities.

facebook/PNPITMS issd.itms@pnp.gov.ph itms.pnp.gov.ph 723-04-01 local 6555

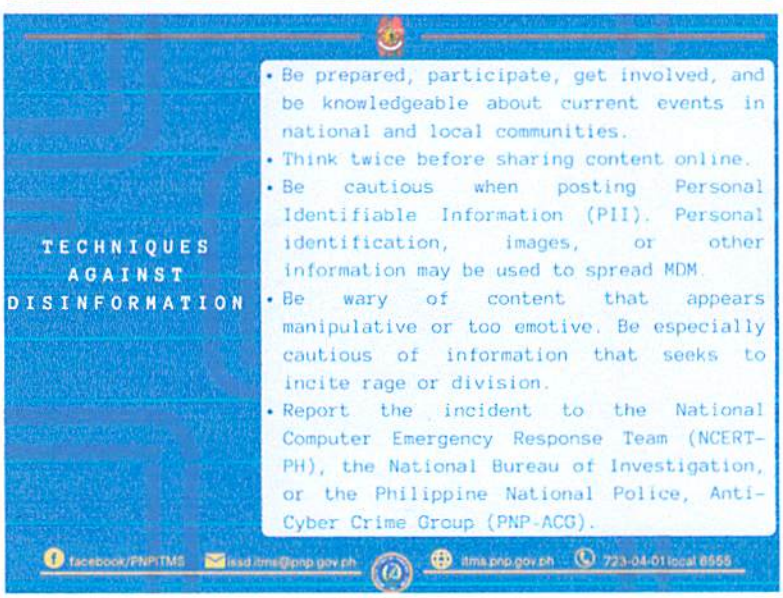
MISINFORMATION, DISINFORMATION AND MAL-INFORMATION

MISINFORMATION	DISINFORMATION	MAL-INFORMATION
a false, but not created or shared with the intention of causing harm.	a false information that is deliberately created to mislead, harm, or manipulate a person, social group, organization, community or country.	an information that is based on fact, but used out of context to mislead a person, social group, organization, community, or country.

facebook/PNPITMS issd.itms@pnp.gov.ph itms.pnp.gov.ph 723-04-01 local 6555


TOOLS USED IN SPREADING DISINFORMATION
Manipulated Audio/Video
audio/video content that captures the public's attention and is repeatedly disseminated. This manipulated content is dangerously effective at spreading false information.
Cheepfakes
are real audio clips and videos that have been sped up, slowed down, or shown out of context to mislead.
Deepfakes
are fake but very believable audio clips and videos crafted and spread to deceive. It can convince that people have said or done things that did not happen.
Forged Artifacts
a common feature that employs forged letterheads, copied and pasted signatures, made-up social media postings, and maliciously edited emails.
Proxy Websites
are fronts for malicious actors, designed to launder disinformation and divisive content or to drive website visits.
facebook/PNPITMS
issd.itms@pnp.gov.ph
itms.pnp.gov.ph
723-04-01 local 6555


TECHNIQUES AGAINST DISINFORMATION
• Confirm its veracity with numerous sources;
• Remain vigilant. Forgeries can be disguised as legitimate content to give them legitimacy. If the forgery appears to be breaking news, check reputable news sites to see if they are covering the event.
• A misspelled URL may indicate that a website is not a reliable source.
• Use multiple fact-checking tools to verify the authenticity and trustworthiness of information.
• Rely on trusted sources such as national and local authority websites and verified authorized social media accounts. Rely on national and local health officials for health and safety updates.
facebook/PNPITMS
issd.itms@pnp.gov.ph
itms.pnp.gov.ph
723-04-01 local 6555


TECHNIQUES AGAINST DISINFORMATION
• Be prepared, participate, get involved, and be knowledgeable about current events in national and local communities.
• Think twice before sharing content online.
• Be cautious when posting Personal Identifiable Information (PII). Personal identification, images, or other information may be used to spread MDM.
• Be wary of content that appears manipulative or too emotive. Be especially cautious of information that seeks to incite rage or division.
• Report the incident to the National Computer Emergency Response Team (NCERT-PH), the National Bureau of Investigation, or the Philippine National Police, Anti-Cyber Crime Group (PNP-ACG).
facebook/PNPITMS
issd.itms@pnp.gov.ph
itms.pnp.gov.ph
723-04-01 local 6555