Security Matters

NEWSLETTER

FACT VS FICTION: INSIGHTS INTO THE WORLD OF DISINFORMATION

Nowadays, anyone with access to social networks, and messaging apps is exposed to receiving and spreading fake news. In addition, these platforms have generated a huge amount of fake content with a tendency to go viral.

Misinformation happens when fake information is shared out of ignorance or by error. Whereas, disinformation happens when fake information is shared on purpose or a reason. Thanks to the advancement of technological progress, from the internet to social media to deepfakes to generative AI, it's becoming increasingly difficult to know whether what we're seeing with our own eyes is real.

Not just our daily lives, elections are likely to face a mix of old and new cybersecurity threats, including phishing and disinformation with the presence of deepfakes and generative AI. Governments and political actors are using AI to generate texts, images, and videos to manipulate public opinion in their favour and to automatically censor critical online content. For example, ahead of the Indonesian elections on February 14, a video of late Indonesian president Suharto advocating for the political party he once presided over went viral. The AI-generated deepfake video that cloned his face and voice racked up 4.7 million views on X alone. Deepfakes are certainly one of the most concerning products of the generative AI revolution. It's now very easy to make it appear as if anyone is saying or doing anything, even things they would never be likely to do in real life.

Disinformation violates the right to accurate information, endangers citizens on issues of public interest, such as climate change or gender equality, and encourages wrong decisions based on manipulated information. It affects the right to freedom of expression, the right to hold opinions without interference, the right to privacy, and the right to participate in public affairs. It directly diminishes the quality of democracy.

These are some channels on which misinformation and disinformation spreads:

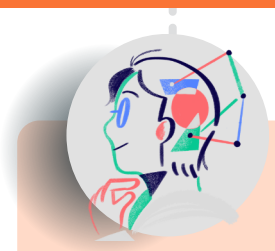
Social media platform: Facebook, X, TikTok, Instagram
Messaging Apps: Telegram, WeChat, WhatsApp
Phishing: Impersonation of authoritative media, people or governments (through false websites and/or social media accounts)
Deepfake technology: Refer to synthetic media generated using deep learning techniques. It can create highly realistic images, audio, and videos that are convincingly manipulated and difficult to detect with the naked eye.
Generative AI: Refers to algorithms that can generate new data based on patterns learned from existing data. This includes text, images, fabricated videos, and audio generation. It can be used to automate the creation of fake news articles, social media posts, or comments that mimic human language patterns.
Bot networks: Social media accounts operated by computer programs, designed to generate posts or engage with social platforms' content.
Traditional media: Oftentimes, the media is used to make fake news more reliable. Some outlets know that they are publishing fake news but still do so due to some sort of benefit. Meanwhile, some do not know that they are publishing fake news.

The world is already affected by misinformation and fake news. With everyone able to use technology, how will we ever know if anything we see or hear is real or not? What can we do to combat the disinformation? Stopping the creation of fake news will probably not be possible. However, we can take action to reduce the damage.

Tips for you: How to spot disinformation?

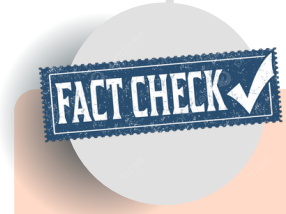
Understand the signs and patterns of disinformation

- Post that making extraordinary claims.
- Using facts from unknown/unreliable sources.
- Story/news that triggered a strong emotional response.
- Mixing fact and opinion in the same stories.
- Using out-of-place pictures or graphics.
- Manipulated video or audio like deepfakes.
- Fake news stories connected with internet scams and "get to rich quick" schemes.
- Misinformation related to vaccination and health such as miraculous remedies.
- News that intentionally created conspiracy theories or rumors such as punching political agendas or discrediting political opponents.



Critical thinking: Strategies for evaluating sources and questioning information

- Who is the author? Are they real?
- How current is the source and where does it come from?
- Who shared the post?
- Why was this shared? (Use your critical mindset)
- Does the headline match the content?
- Is the content made up of facts or opinions?
- What is the supporting evidence?
- Could it be a joke?
- How authentic is the post/images/source?
- Does it create distrust or discrimination?
- How did the post make me feel? (Check-in your emotion and own belief system)



Recommended fact-checking resources/platforms for verifying information

Malaysia: Malaysiakini, Sebenarnya.my, MyCheck Malaysia, JomCheck Malaysia

Thailand: Co-Fact, AFP Fact Check, Fact Crescendo, Sure and Share Center

Indonesia: CekFakta, Mafindo

Vietnam: VietFactCheck

Cambodia: CamBoJA

Myanmar: Fact Crescendo

More...

- Check the URL as some fake news sites will use a web address designed to make it look like a real news source.
- Beware of your emotions. If it triggers a lot of emotions inside you, always check the story with another reputable source.
- Sharing accurate information responsibly.
- Cultivate media literacy education and digital citizenship.
- Supporting initiatives aimed at countering disinformation.
- Report any suspicious posts or profiles that contain misinformation/disinformation to the respective channel/party.

Related News

This dangerous Android malware is pretending to be a McAfee security tool

Stay alert, hackers are tricking people into installing fake McAfee antivirus software. A new version of a known Android banking trojan is making rounds on the internet, stealing sensitive data, and possibly even money, from its victims.
Read more: https://bit.ly/45aF9iW

A group is battling fake news one conversation at a time in Taiwan

Like any democratic society, Taiwan is flooded with assorted types of disinformation. Despite its very public nature, disinformation has a deeply personal impact – particularly among Taiwan's older people. It thrives in the natural gaps between people that come from generational differences and a constantly updating tech landscape, then enlarges those gaps to cause rifts.
Read more: https://bit.ly/47BjGB8

Ransomware attackers are increasingly targeting backups

Hackers know the importance of backups in a ransomware attack. When deploying ransomware on a target system, threat actors will almost always look to compromise the backups, too. Organizations that lose their backups end up paying a lot more in ransom demands, and losing even more in the recovery process,
Read more: https://bit.ly/3wr7cOr

Only 2% Malaysian organisations are ready against cybersecurity threats

The American IT and networking firm Cisco Systems has revealed that a mere 2% of all organisations in Malaysia are ready enough to be resilient against modern cybersecurity risks. About two thirds of all Malaysian organisations are also only either now starting to deploy or currently have below average security readiness to deal with threats.
Read more: https://bit.ly/3wr7cOr

Malaysia passes Cyber Security Bill 2024

The Dewan Negara Malaysia passed the Cyber Security Bill 2024 on April 3. The aim of the bill was to enhance the nation's cyber security through compliance with specific measures, standards, and processes in managing cyber security threats. It could help the government ensure the viability and efficiency of the Critical National Information Infrastructure (CNII) in handling cyber security incidents.
Read more: https://bit.ly/3wr7cOr

General Helpline: help@securitymatters.asia
Secure Communication via Protonmail: secmhelpdesk@pm.me

More information about Security Matters, visit www.securitymatters.asia
info@securitymatters.asia
@secm8 @sec_matters

Visa warns dangerous new malware is attacking financial firms

Visa is warning its partners, clients, and customers, of an ongoing phishing attack that aims to deliver a banking trojan. The campaign targets mostly financial institutions in South and Southeast Asia, the Middle East, and Africa, and aims to drop a new version of the banking trojan called JsOutProx.
Read more: https://bit.ly/3Q6CJge

Gmail and YouTube hackers bypass Google's 2FA account security

Hackers are taking over accounts despite two-factor authentication (2FA) protection. Desperate Gmail and YouTube users are turning to official and unofficial Google support forums after hackers take over their accounts, bypassing 2FA security and then locking them out.
Read more: https://bit.ly/3HZme0n

Banks will never request this information over the phone

The Association of Banks in Malaysia (ABM) and the Association of Islamic Banking and Financial Institutions Malaysia (AIBIM) have jointly issued a reminder to warned bank customers who suspected that they may have received a call from fraudsters impersonating bank officers should immediately hang up and call the bank's official customer service hotline instead.
Read more: https://bit.ly/4bCCfqQ

LightSpy malware attacking Android and iOS users

A new malware known as LightSpy has been targeting Android and iOS users.This sophisticated surveillance tool raises alarms across the cybersecurity community due to its extensive capabilities to exfiltrate sensitive user data.
Read more: https://bit.ly/48lucMe

Google ad for Facebook redirects to scam

How can Google differentiate a legitimate affiliate from a malicious actor? There are a number of data points about the advertiser via their account: user profile, payment method, budget, and there is the ad itself like vanity URL, display text, tracking template, final URL. What happens when you click on the ad? Are you actually redirected to the URL claimed in the ad?
Read more: https://bit.ly/48lihhA