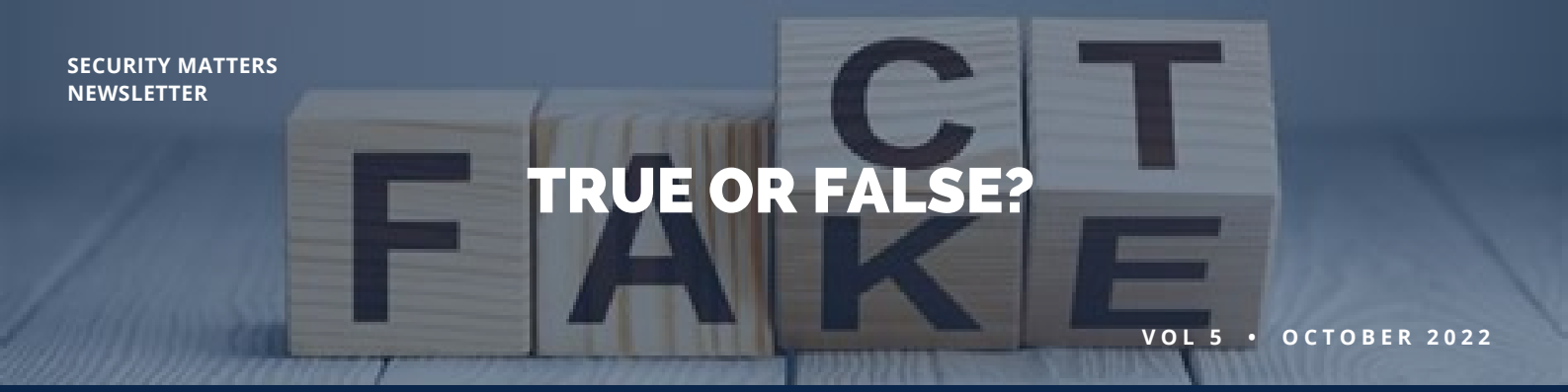
SECURITY MATTERS
NEWSLETTER



TRUE OR FALSE?

VOL 5 • OCTOBER 2022

What we should keep in mind when researching information on the internet? Not all sources are reliable. Misinformation happens when false information is shared out of ignorance or by error. Whereas, disinformation happens when false information is shared on purpose or a reason. Disinformation can be propagated by a host of online actors, including governments, extremist groups, and individuals. It's commonly spread through messaging apps, social media, streaming video outlets and 'fake' news sites.

Political disinformation is not new in Southeast Asia and each country have different disinformation landscapes. During election cycles, voters are also bombarded with disinformation that is difficult to distinguish, false conspiracy theories and propaganda from illegitimate sources. Now we're seeing more sophisticated disinformation/misinformation campaigns that include deep fakes, chain messages and phishing scams. These fake information are being used to deliver malware by manipulating people's fears and heightened emotions. Let's check out some of the sign and examples of disinformation here:

Sign / Examples of disinformation

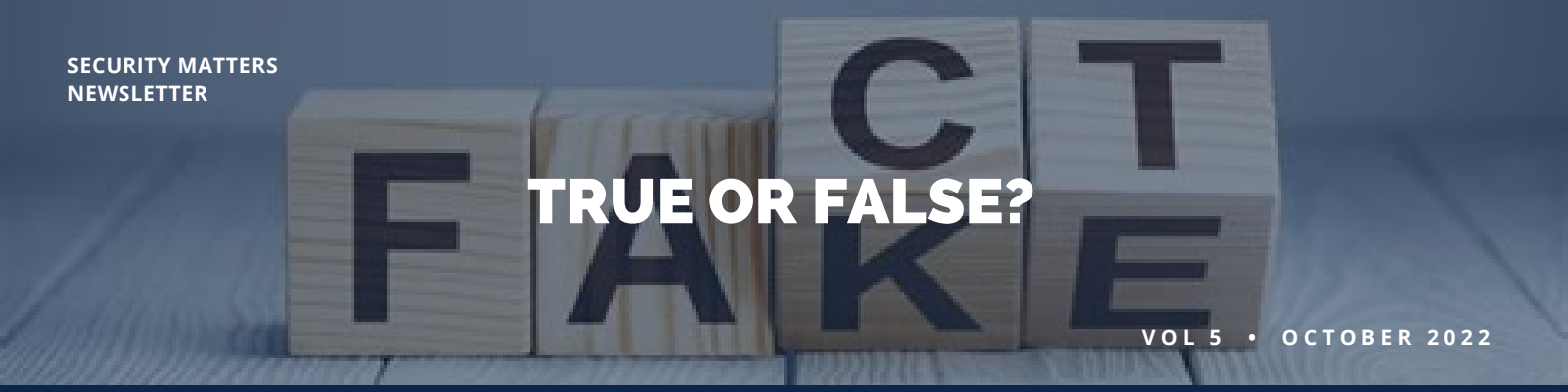
- Post that making extraordinary claims.
- Using facts from unknown/unreliable sources.
- Story/news that triggered a strong emotional response.
- Mixing fact and opinion in the same stories.
- Using out-of-place pictures or graphics.
- Manipulated video or audio like deepfakes.
- Fake news stories connected with internet scams and "get to rich quick" schemes.
- Misinformation related to COVID-19 and vaccination such as miraculous remedies.
- News that intentionally created conspiracy theories or rumors such as punching political agendas or discrediting political opponents.

SECURITY MATTERS

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

SECURITY MATTERS
NEWSLETTER



TRUE OR FALSE?

VOL 5 • OCTOBER 2022

How to identify disinformation?

- Analyze both the contents and sources.
- Identify whether the information is misinformation or disinformation.
- Try to identify the intend behind the post or information.
- Use authoritative resources.
- Evaluate how the information fits into your own belief system.

Ok, disinformation/fake news spotted. Now what?
DO NOT share or amplify it in any way, even if it's to correct or debunk the false claim.
Sometimes, sharing is not caring.

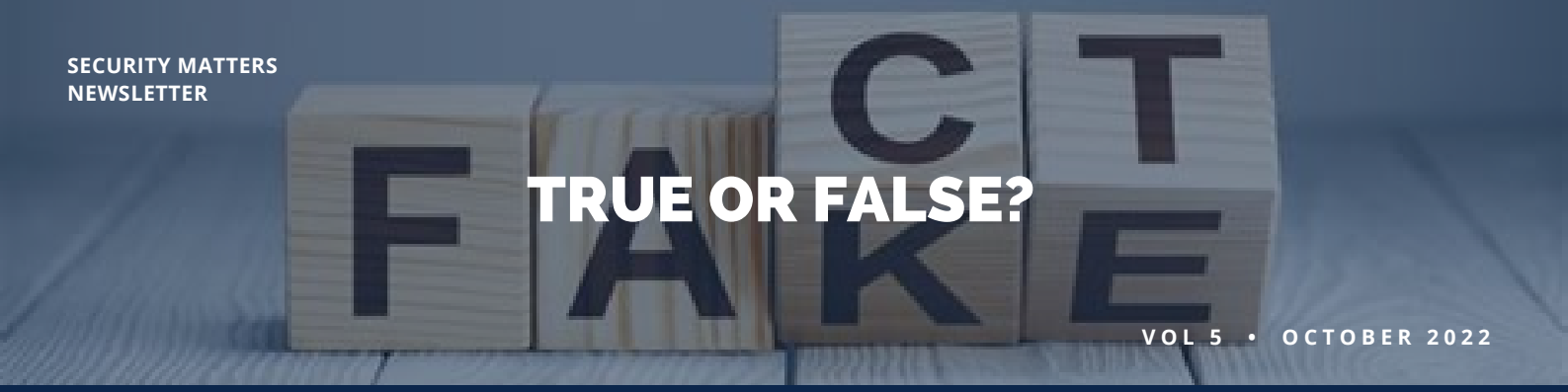
CHECKLIST

- [ ] Who is the author? Are they real?
- [ ] How current is the source and where does it come from?
- [ ] Who shared the post?
- [ ] 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?
- [ ] Have I cross-referenced from fact-checking sites for verification?
- [ ] Does it create distrust or discrimination?
- [ ] How did the post make me feel? (Check-in your emotion and own belief system)
- [ ] Why was this shared? (Use your critical mindset)

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

SECURITY MATTERS
NEWSLETTER



TRUE OR FALSE?

VOL 5 • OCTOBER 2022

How to prevent and stop the spread of disinformation?

Educate yourself. Learn to identify misinformation and disinformation.

Recognize the risk and vulnerabilities. Always check the source, the author, published date, content, pictures and videos to identify its authenticity level.

Consider the source. Always questions the source of content and their intent behind, investigate the issues/claims before sharing. Use a fact-checking sites to verify a claim.

Watch out for spoofed domains. Check the URL as some fake news sites will use a web address designed to make it look like real news source.

Beware of your emotions. If it's trigger a lot of emotions inside you, always check the story with another reputable source.

Be critical of information that fits into your belief system. If a claim/post fits into your biases, it can be easy to spread information that feels right to you.

Be skeptical of outrageous claims that seem unbelievable.

Voice out. Stand up to disinformation privately or publicly although it may feel uncomfortable to face challenge or conflict.

Report any suspicious posts or profile that contain misinformation/disinformation to the respective channel/party.

We all have the ability and responsibility to limit the spread of disinformation.
Let's work together to keep our society safer and slightly more trustworthy.

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

Related News

Uninstall these malicious mobile apps now, Facebook warns

Facebook identified more than 400 malicious Android and iOS apps this year that target people across the internet to steal their Facebook login information. These apps were listed on the Google Play Store and Apple's App Store and disguised as photo editors, games, VPN services, business apps and other utilities to trick people into downloading them.
Read more: https://bit.ly/3fMmmFI

Digital rights activists in Southeast Asia increasingly at risk

Online censorship, digital surveillance, and harassment have become the daily norm for many young human rights defenders and activists in Southeast Asia. Those who speak up online are increasingly having to contend with the digital as well as physical threats that activism often comes with, human rights experts say.
Read more: https://bit.ly/3VH2UuF

Now finger heat can crack passwords with the help of AI

A group of researchers discovered that Hackers can use finger heat to crack passwords now all with the help of Artificial Intelligence technology by using a system ThermoSecure where a thermal camera is used to recognize the touch on the keys made by an individual.
Read more: https://bit.ly/3Vl7luM

Fake Tor browser installer spreading malware via YouTube

Cybersecurity researchers have discovered multiple infections through a malicious TOR browser installer. The shady YouTube video is spreading a modified version of the TOR browser capable of collecting sensitive data from users in China. This includes internet history and data the user enters into website forms.
Read more: https://bit.ly/3yvMhs0

Zoom phishing scam steals Microsoft Exchange credentials

A new phishing attack revealed in which scammers spoofed Zoom users to steal their Microsoft Exchange credentials. The phishing email, which was marked as safe by Microsoft, was aimed at 21,000 users of a national healthcare firm.
Read more: https://bit.ly/3EAcSrq

WhatsApp users beware: Dangerous mobile Trojan being distributed via malicious mod

Users who download YoWhatsApp, a modified version of the WhatsApp app are at risk of having their WhatsApp account details stolen and being signed up for paid subscriptions they did not want or were even aware of.
Read more: https://bit.ly/3g0aW1b

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

Related News

Android device leaks traffic when connected to WiFi network even 'always-on VPN' is enabled

It was discovered that every time an Android device connects to a WiFi network, it leaks traffic and this leak happens after enabling the security features like 'Always-on VPN' and 'Block connections without a VPN '.
Read more: https://bit.ly/3CWT8Nx

A closer look at the National Scam Response Centre Malaysia

The Malaysia's government has set up the National Scam Response Centre (NSRC) to deal with a growing number of cyber fraud cases in the country. It focuses on online financial fraud, including phishing scams, Macau scams, malware attack scams, parcel scams and love scams.
Read more: https://bit.ly/3CxP1Gn

Signal kills support for SMS texting due to lack of privacy

Signal decided to part with SMS support because messages sent via the Signal interface on Android cannot be protected to the level of the company's privacy standard. Anyone who is not sure what they are using to send their SMS can check this in the Signal settings under "Conversations/SMS and MMS/Use as default SMS app.
Read more: https://bit.ly/3EV3KOe

Contenting with spyware and oppression in Thailand

Apple and Facebook have filed lawsuits against NSO over the Pegasus technology. But while the company claims it has turned down many customers over ethical concerns, activists and human rights defenders around the world continue to be targeted, with especially dire consequences in authoritarian states or countries where democracy is weak or precarious.
Read more: https://bit.ly/3Se1cxY

Internet freedom remained under threat in Indonesia

The government critics, journalists, and ordinary users in Indonesia continued to face criminal charges and harassment in retaliation for their online activity and reporting. After the coverage period, authorities escalated their efforts to force technology companies to comply with a law that imposes take down and registration requirements, briefly blocking some platforms.
Read more: https://bit.ly/3CYor9M

Internet freedom remained restricted in Malaysia in 2022

The government blocks websites and orders content removed over political or religious sensitivities. Criminal prosecutions and investigations for social media posts and other forms of online expression also threatened internet freedom. Users, particularly those from the LGBT+ community, continue to face online and offline harassment for their online posts.
Read more: https://bit.ly/3gzpzZM

SECURITY MATTERS

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