Case Study: OSINT Misidentification During COVID-19 (Singapore, 2020)

In May 2020, during Singapore’s COVID-19 pandemic, the government had implemented a mask mandate. A woman was filmed not wearing a mask in public, which was a breach of the regulations.

Amateur investigators on social media used **open source intelligence (OSINT)** techniques to try to identify her. Within hours, they publicly claimed she was the CEO of a digital security firm. They also shared the names and photos of her alleged employees.

What Happened

- The woman identified by social media users was **not the actual person in the video**.
- Despite this, the social media posts had already spread widely.
- The falsely accused CEO received **racist comments, harassment, and threats** online.
- The company suffered **reputational damage and a loss of business** as a result of the viral misinformation.

Consequences

1. **Personal harm:** The wrongly identified woman faced harassment, threats, and emotional distress.
2. **Professional impact:** The company’s reputation and operations were damaged.
3. **Legal and ethical issues:** Spreading unverified personal information online can lead to defamation, harassment, and potential legal liability.
4. **Misinformation amplification:** The speed of social media sharing meant the false identification spread before corrections could be made.

Lessons Learned

- **OSINT can be misused:** Even publicly available information, if interpreted incorrectly, can cause serious harm.
- **Verification is crucial:** Claims about personal identity must be confirmed before sharing online.
- **Privacy and ethics matter:** Sharing personal details without consent is both unethical and potentially illegal.
- **Rapid response needed:** Organisations should have protocols for managing false accusations online.
- **Education:** Social media users should be aware of the dangers of “amateur sleuthing” and the potential consequences of spreading unverified information.