You get a call from an unfamiliar number. The person on the line claims to be a police officer informing you that you are wanted for money laundering. They recently arrested a suspect who named you as an accomplice.

Phishing scams must be a nightmare. You must have been a victim or a family member. Someone has been compromised and now you are being framed. The ‘officer’ then offers to help you prove your innocence. You agree, and the scam begins.

**Anatomy of a scam**

**Understanding and avoiding phone and online scams.**

**Macao scam** - The scammer would pose as an authority figure, usually a police officer, bank officer or government official over the phone. The victim would be told they have some kind of criminal conviction against them. There are also cases of callers pretending to be a representative of a telecommunications company, calling to claim a long outstanding bill or false legal action. They may claim to have kidnapped your family member, and demand ransom, or told the victim they have lottery winnings to claim. The ultimate aim is to get the victim into a heightened emotional state, so they can be talked into revealing personal banking information or handing over money.

**Love scam** - Sometimes known as a postal scam, scammers usually connect with their targets via social media or dating sites and apps. They would begin to distance or reassure the target. Once a relationship is established, the scammer would entice the victim with promises of gifts in the mail. An accomplice would then contact the victim, posing as a government officer or courier staff claiming the package has been delayed by authorities for inspection. The victim is required to pay money to have the parcel released.

**Decoding the Scammers’ Modes of Operations**

Let’s look at three of the most common phone and online scams, and why they work:

- **Bogus offers** - With the world battling the COVID-19 pandemic, the CCD said early April that there have been a total 516 cases of scams involving the sale of fake masks or and online platforms in Malaysia, with losses amounting to RM42 million.

  The majority of these cases occurred during the Movement Control Order (MCO) that started on 18 March. As of April 2020, there were 516 cases of Scams involving the sale of fake masks or and online platforms in Malaysia, with losses amounting to RM42 million.

- **Bogus job opportunities** - Scammers use the current job market to entice victims with promises of high pay jobs or opportunities that require no experience or qualifications.

 前に述べたように、セーラーの不道徳な行動は多数ある。決定的な手段は、警察官の名目で、偽のメールを送り、被害者に転売される場合がある。この偽メールには、日常の情報で、警察官の名目で、偽のメールを送る側も、偽のメールを受信する側も、被害者になる可能性がある。