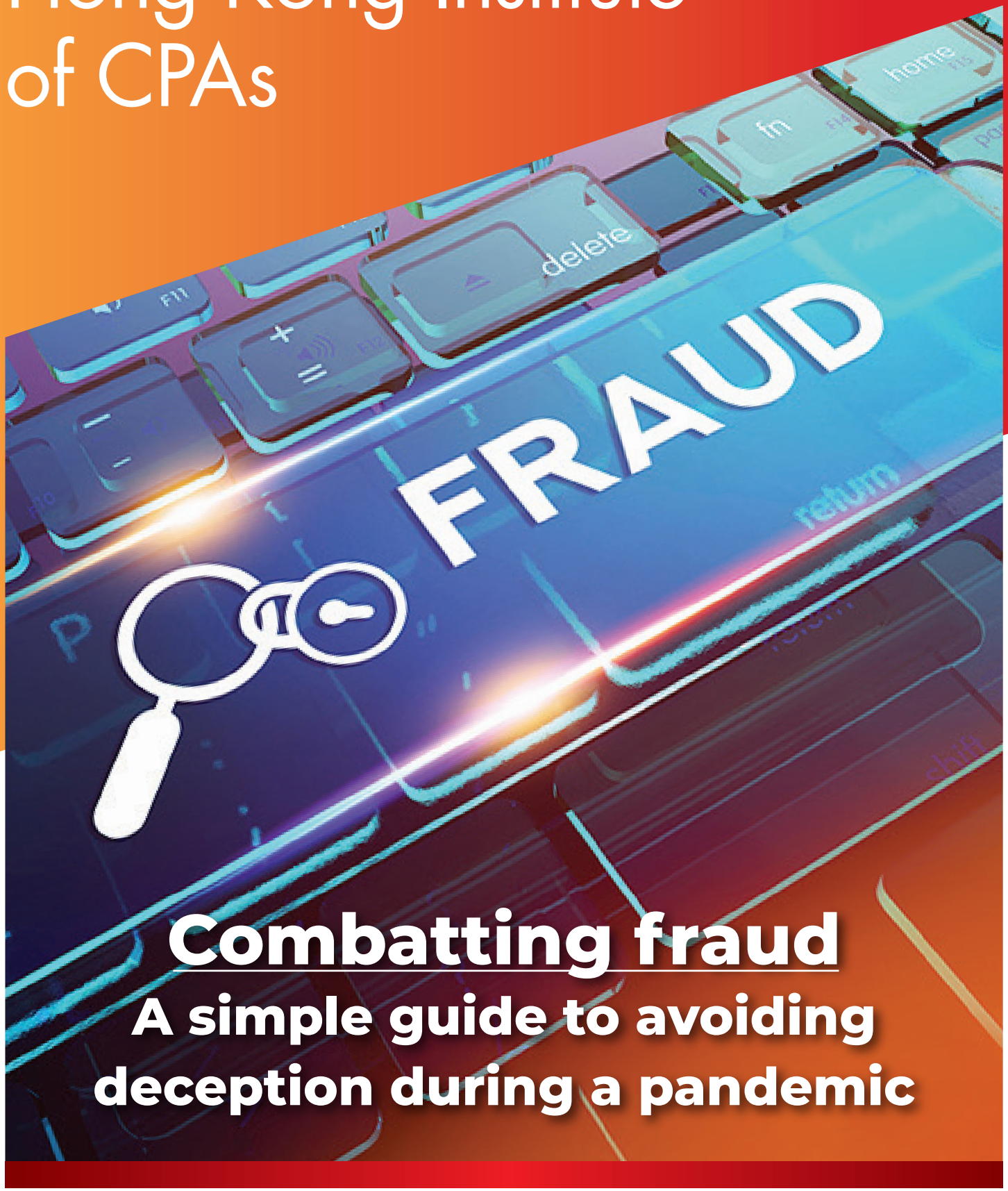
Hong Kong Institute of CPAs



Combatting fraud

A simple guide to avoiding deception during a pandemic

CPA
Hong Kong Institute of
Certified Public Accountants
香港會計師公會

COVID-19 is unprecedented in modern times and continues to disrupt people's lives and economies around the world. Social distancing measures have been implemented globally, including in Hong Kong, to contain the spread of the pandemic. During these extraordinary times, it is especially important to remain alert in order to protect your and your family's health and also your hard-earned assets. Opportunistic criminals will quickly find way to use new situations to exploit vulnerable and unwary members of the public to enrich themselves through various kinds of scams.

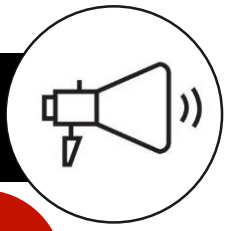
This guidance from the Hong Kong Institute of Certified Public Accountants' Forensics Interest Group Management Committee includes some commonly-seen deceptions and frauds, which are not exclusive to the present situation, as well as some possible measures to combat such scams. Please note that this is not an exhaustive list of possible scams. Individuals should be on heightened alert for attempts by fraudsters to take advantage of opportunities arising from remote working and other aspects of the current health and economic situation.

Fake domain and phishing scams

Fake Internet domain names and websites may be set up to closely resemble those of official organizations, such as the World Health Organization (WHO), e.g., the address <who.intgov>, which looks like the official domain name <who.int>. These fake domain names can be used in “phishing” emails which, when opened, may attempt to steal the users’ personal information and data or engage in other types of deception. The links may download malicious software onto your device, which may not easily be detectable afterwards. With such software, fraudsters may be able to harvest sensitive data, e.g. credit card numbers and passwords, and access accounts or sell user information.

What should you do?

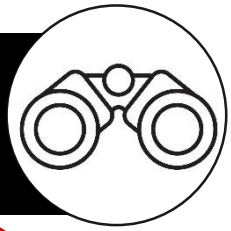
Updated alerts and policies should be provided to staff in view of the global and local developments



Staff within an organization should be alerted and kept up to date about potential frauds arising from the COVID-19 situation. Organizations should:

- Set up an effective reporting system, through which possible fraud cases can be reported quickly to relevant personnel;
- Develop a contingency plan, which should be reviewed and updated periodically, providing step-by-step guidance to deal with possible scams; and
- Designate appropriate professional staff, such as forensic accountants and investigators, cybersecurity experts and lawyers, with relevant expertise and experience, to provide support and advice.

Be wary of emails, particularly those not directly related to your work from an unfamiliar source, which appear to require your immediate action

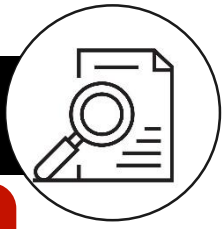


These emails may be associated with a reward for acting, or risk of not acting, quickly, aiming to lure you to click on a link and provide personal information. Instead, stop, think and talk to your employer's information technology staff. Do not click on embedded links and, if in doubt, delete the message.

Disregard unsolicited email/telephone requests, apparently from government agencies, financial institutions, etc. asking for personal information

Do not respond to unsolicited emails or telephone calls by acceding to requests/demands to provide your personal data. It is highly unlikely that legitimate government agencies, banks, etc. will request/demand that information. If in doubt, consider contacting the relevant agency or institution directly to confirm whether they are the source of the email or telephone call. If you do so, you should find the authentic contact details of the relevant organization from a trusted source and should not use any link in the email or ask to speak to another colleague of the caller while on the same telephone call.

Observe whether communications contain spelling and grammatical mistakes



If an email includes spelling, punctuation, and grammatical errors, it is a common sign you have received a phishing email.

Be wary of generic emails that do not address you by name

Email greetings which do not address you by name, but merely as “Sir or Madam”, may suggest that the email is one to avoid.

Check the email address or link

If you are unsure, you may wish to double check the relevant links in the email by, e.g., copying the link address and pasting it into the “Search” function of a search engine, such as Google. If you are not directed to an authentic website, the email is almost certainly a phishing email. However, it is still necessary to be cautious as the link address may take you to a lookalike fake website. Another regular scamming tactic involves an email apparently from a known source, contact or friend but with an unfamiliar domain name (e.g. JohnWong@xbrzbyly.com). Emails of this type should just be deleted. Do not respond to them.

Change compromised usernames and passwords

If you think your login name and, more importantly, your password, has been obtained by third parties, who may be fraudsters, you should consider changing this sensitive information as soon as practicable. If your password is quoted in the title or body of an email, this is clear evidence that it has been obtained illegitimately and should be changed. Ensure that any new passwords are strong, and not just a slight variation on a compromised password.

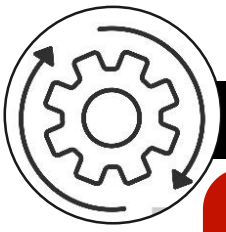
Impersonation fraud

With many people working from home, fraudsters may take this opportunity of physical distancing to impersonate a colleague or member of the senior management of your employer to deceive you into, e.g., making a fund transfer.

What should you do?

Verify the source of requests to complete transactions

It is important to stay vigilant, particularly in a situation where you are requested or instructed to complete an important transaction through an unexpected telephone message or email. You should consider contacting your supervisor, or colleagues in internal control and risk management, internal audit, or forensic services, as appropriate, for confirmation or clarification. You may also consider checking whether it is legitimate by telephoning/ emailing back to the person purportedly making the request, after confirming the correct phone number/ email address from your employer's internal phone directory/ email address book.



Update your software

You should use a secure, password protected wi-fi system and run anti-malware and anti-virus software to prevent your personal devices from being hacked. As far as possible, ensure that this protection software is up to date by downloading the latest security patches. Avoid using unsecure public systems for sensitive and important internal communications.

Keep up to date with the latest scams

If you are not sure about particular email, telephone message or cold call, you may want to check reliable sources for the latest scamming tactics (e.g., government and regulators' cybercrime websites, such as the "Useful links" on P. 8).

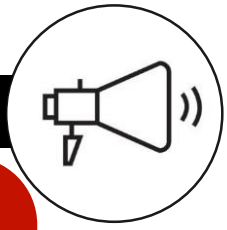
Product fraud

Some scams involve attempting to sell products which, e.g., claim to prevent or cure COVID-19, or invest in companies that have created a vaccine or discovered a cure.

However, there is no known cure or vaccine as yet, and no treatment known to be 100% effective. As with other situations of significant uncertainty, there is a great deal of misinformation and speculation circulating on the Internet and through social media, some of it with deliberate intent to mislead or defraud. In practice, it is expected to be many months, or even years, before a safe and effective vaccine to combat COVID-19 may be developed and made widely available.

Other scams may induce people to purchase non-existent or substandard personal protective equipment.

What should you do?



Read a company's announcement

If you receive a cold call to ask you to invest in, or purchase, a product such as a new vaccine or drug, developed by a listed company, which can cure COVID-19, you should check whether this has been reported in the company's formal public announcements placed on the relevant listing authority's platform (such as the platform of the Hong Kong Stock Exchange). You can then check any announcements against promotional material supposedly from the company or its agents. It is always safer to be sceptical and observe whether there are any inconsistencies between the information provided by the caller and company announcements.

Verify the underlying information

You should conduct proper due diligence research before deciding to invest in a company that claims to have developed, or be close to producing a COVID-19 vaccine, including whether the company has a proper track record of developing vaccines, or in related medical fields. Fraudsters may tell a convincing story to lure you into a making a quick and lucrative investment "ahead of the crowd".

It is prudent to remain sceptical about exclusive potential investment opportunities and stories that sound too good to be true, bearing in mind that reputable research organizations/ companies do not make cold calls to seek investment.

Financial statement frauds

Some companies could be under pressure to manipulate their performance figures due to the pandemic, to show that they are able to navigate through the crisis and still make reasonable profits.

Potential frauds may include overstating of revenues, understating of operating expenses, or converting expenses into capital expenditure, manipulating the valuation of assets, etc.

What should you do?

Check for red flags

As a potential investor in, or a business partner of, a particular company, you may want to pay attention to the following red flags to avoid being lured into dealing with a suspect company. Look at whether:

- The company's financial performance far exceeds its competitors in the industry. If yes, what kind of business strategies have been adopted that could explain this?
- The company has maintained consistent gross profit margins while its industry is facing pricing pressure.
- Revenue growth is in line with the company's cash flow.
- There is an unexpected accumulation of fixed assets, implying that some operating expenses may have been capitalized.
- There are unforeseen related party transactions?
- There are negative and plausible analyst/ short seller reports about the company.

Useful links

GovHK – Technology Crime:
https://www.gov.hk/en/residents/communication/infosec/technologycrime.htm

Hong Kong Monetary Authority – Beware of Fraudsters:
https://www.hkma.gov.hk/eng/smart-consumers/beware-of-fraudsters/

The Hong Kong Police Force – Cyber Security and Technology Crime:
https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/index.html

Investor and Financial Education Council – Beware of Online Scams:
https://www.ifec.org.hk/web/en/moneyessentials/scams/scam-websites.page

Hong Kong Institute of Certified Public Accountants
37th Floor, Wu Chung House
213 Queen's Road East, Wanchai, Hong Kong
Tel: (852) 2287 7228
Fax: (852) 2865 6603
Email: hkicpa@hkicpa.org.hk
Website: www.hkicpa.org.hk