

識別及防止 2019 冠狀病毒虛假訊息

由流言以至假數字，有關 2019 冠狀病毒的虛假訊息都不斷在網上瘋傳。而網絡保安公司亦指出，利用 2019 冠狀病毒疫情進行的網絡攻擊亦已大為增加，其手法大都是誘騙受害者點擊連結往被入侵網站或下載惡意程式，從而窺視或偷竊受害者的個人資料。監察機構亦發現越來越多網站在推廣一些未經驗證的醫療建議或治療方法。請參考以下提示以保護自己及家人，讓大家保持消息靈通，防止網上歹徒及虛假訊息發佈者得逞。



識別：

經常保持警惕及了解可能的詐騙行為及醫療健康騙局

- ✓ 應審慎對待從網上得來的訊息。假如您和您的家人都在花費更多時間上網、瀏覽社交媒體及收取更多有關 2019 冠狀病毒的電郵，您們都應該更嚴謹地了解、信納及分享這些訊息，並確保每位家庭成員都採取同一態度。
- ✓ 分析訊息的語氣。假如一個訊息使用誇張的語言，例如所有內文都用大楷來寫，其可信度可能極有疑問。
- ✓ 小心一些依賴傳言或個人意見來推廣某些醫療方法的訊息，而這些醫療方法通常都好得令人難以置信。
- ✓ 特別小心一些請求保守秘密或施壓鼓勵馬上行動的要求。
- ✓ 查核 NewsGuard 的 2019 冠狀病毒虛假訊息即時報告，以認識有關 2019 冠狀病毒的常見謬誤及將這些訊息歸類為虛假的原因：<https://www.newsguardtech.com/covid-19-resources/>。

核實：

經常核實訊息來源及質疑網上資料的合法性

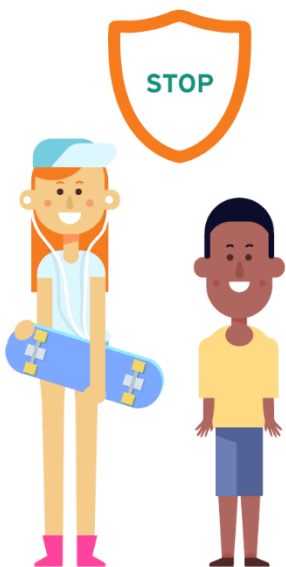


- ✓ 經常核實所看到的資料是直接來自一個可靠的來源，嘗試只從權威渠道取得 2019 冠狀病毒的最新資訊，如世界衛生組織、疾病預防及控制中心或本地政府組織。
- ✓ 假如您不肯定訊息的來源是否可靠，您可以從其他資料來源覆查同一內容以確定資料的可靠性。
- ✓ 仔細審查所有提出轉賬指示的電郵要求，特別是在此類要求並不常見的情況下。
- ✓ 教導自己及子女對所接收資訊提出疑問，美國 [National Association for Media Literacy Education](#) 建議的問題包括：

- 為甚麼要製作這資訊或文章？
- 這資訊遺漏了甚麼資料？
- 誰人製作了這資訊？
- 有誰會從這資訊得益？
- 我如何知道這資訊是真的？
- 有誰會被這資訊傷害？

阻止：

盡責任防止網上詐騙及虛假訊息發佈



- ✓ 分享來自可靠來源的真實及最新 2019 冠狀病毒資訊，以踢走虛假資訊。
- ✓ 假如您看到朋友分享不實的資訊，可以禮貌地告知事實，並為他推介可靠資訊來源。
- ✓ 小心保護自己免受黑客或網絡歹徒利用 2019 冠狀病毒作誘餌攻擊，他們一般都會誘導受害者點擊連結往惡意網站以騙取個人資料，或是下載包含惡意或間諜程式的附件。您應採用具信譽及最新的保安軟件來保護自己及家人。
- ✓ 即時舉報及刪除來源不明的垃圾電郵，切勿打開電郵、點擊內含的連結或打開附件。
- ✓ 鼓勵朋友及家人安裝 [NewsGuard 的瀏覽器延伸程式](#)。它提估數以千計資訊來源的可靠性，有助保護色受不實資訊影響。
- ✓ 如果您發現有網站傳遞 2019 冠狀病毒的欺騙性資訊，而該網站未被 NewsGuard 評級，可發送提示至：<https://www.newsguardtech.com/misinformation-hotline/>。