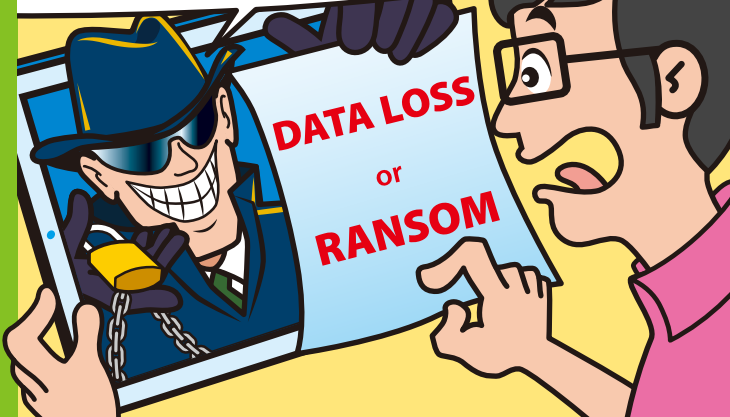


# Smart You Smart Device

Awesome!  
Get pay apps  
for free!



Kekeke... Your device  
has been kidnapped.  
Ransom, please.



Apps from unknown source  
are dangerous, U know?



Of course.



So, I used the "DEMO"  
device to try. Easy to  
guess the device  
password "1234".



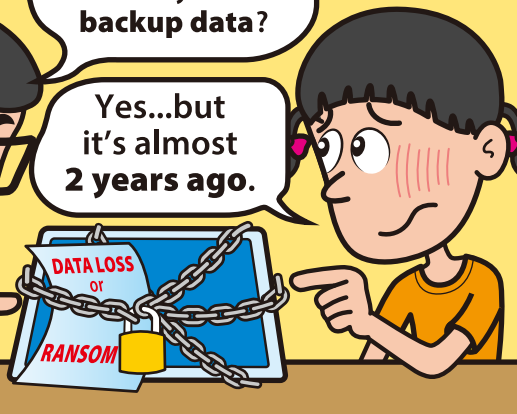
DEMO?  
That's mine.



Did you  
backup data?



Yes...but  
it's almost  
2 years ago.



## Secure Your Mobile Device



Please  follow the security  
good practices below -

- use strong password
- enable security apps to detect malware
- use up-to-date operating system, apps and web browsers
- enable device encryption
- remove unnecessary connection settings
- restrict installation of mobile apps from unofficial sources
- examine the permission requests of apps before installation
- backup data regularly
- stop location service if not necessary



# 精明用家 智能裝置

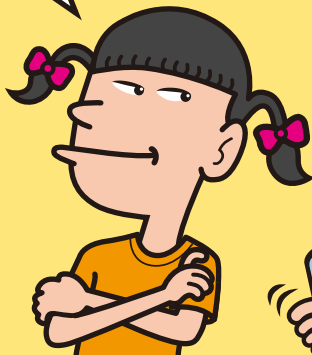
咦?! 唔使俾錢就可以  
安裝到要收費嘅軟件!



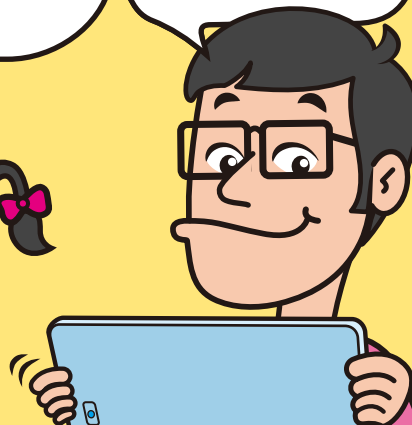
咕咕咕... 你嘅裝置已經  
被綁架喇! 唔該俾贖金  
啦!



來歷不明嘅軟件好危險  
㗎, 你知唔知呢?



我梗係知道啦!



所以我咪用部“DEMO”機  
去試裝囉。個裝置密碼  
係“1234”咁嘛!  
好易估啫!



DEMO?  
部機係我㗎!

你有備份資料  
㗎呵?



有就有... 不過係  
兩年前嘅事...

## 保護你的流動裝置



請  遵循以下良好保安守則:

- 使用嚴謹的密碼
- 啓動保安程式以偵測惡意軟件
- 使用最新版本的作業系統、應用程式及互聯網瀏覽器
- 啓動裝置加密功能
- 移除不必要的連接設定
- 限制安裝非官方的流動應用程式
- 安裝前審查應用程式的權限要求
- 定期備份資料
- 不需要時應停止定位服務

