Stay Alert!
Use Wi-Fi Network with Care

Secure Your Wi-Fi Network

Please ☑ follow the security good practices below –

- □ update firmware and software of your devices, such as Wi-Fi routers and TV boxes regularly
- □ avoid using default settings in Wi-Fi routers, such as the default Service Set Identifier (SSID) and administrator password
- □ enable strong security for Wi-Fi communication, such as using WPA2 with AES 256-bit encryption
- □ enable built-in firewall of Wi-Fi router to protect your internal network
- □ turn off your Wi-Fi router if not in use

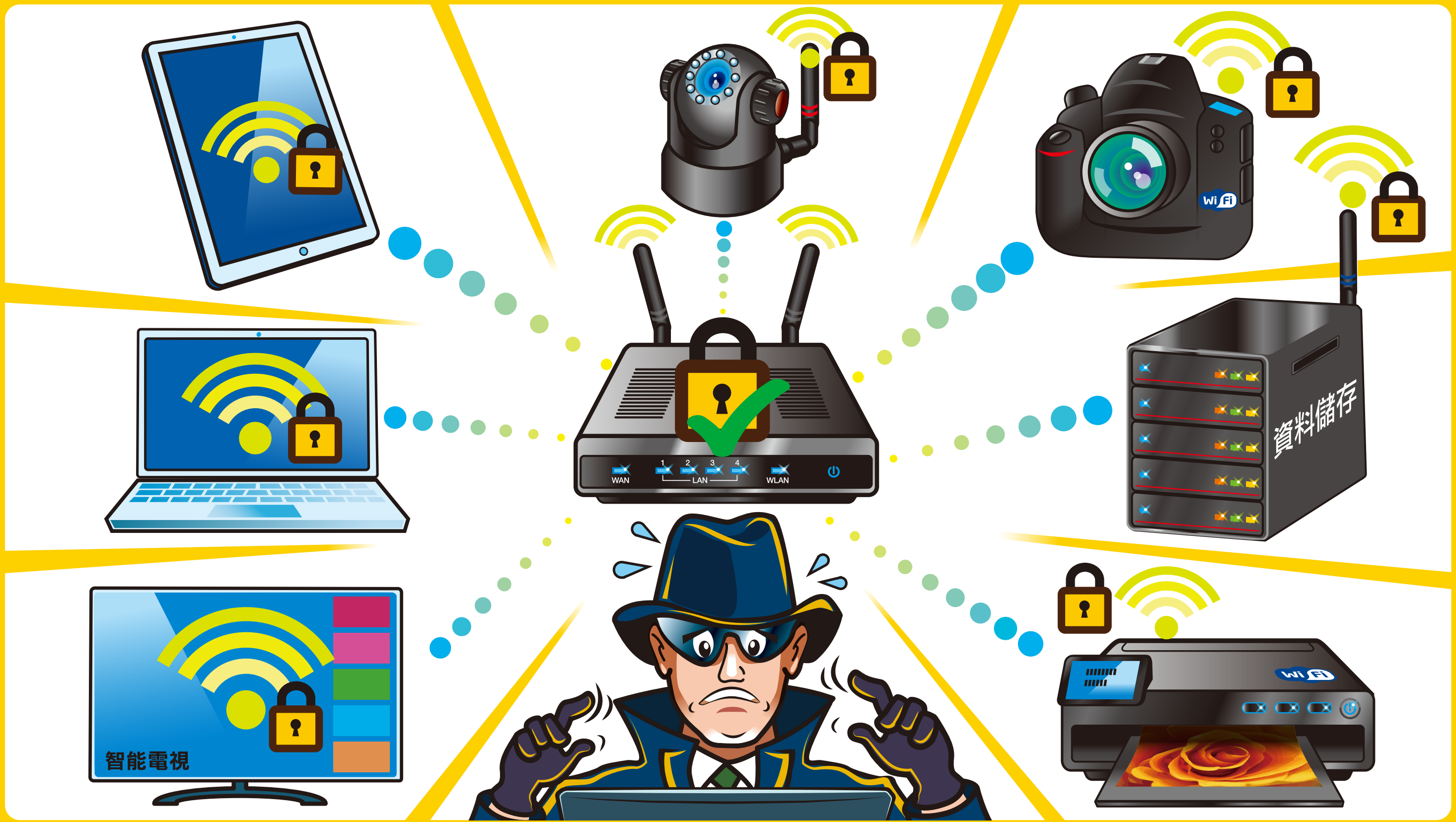
More advice for schools and small and medium enterprises (SMEs) –

- □ formulate policies on the proper use of Wi-Fi network and IT security instructions for end users
- □ enable MAC address filtering or other secure mechanisms for user authentication
- □ position Wi-Fi routers and wireless access points properly
- □ restrict access from guest Wi-Fi network to your internal network
- □ review log records regularly to detect suspicious events

Cyber Security Information Portal
www.cybersecurity.hk

Office of the Government Chief Information Officer

保持警覺！
無線上網 保安勿忘



保護你的Wi-Fi網絡

請 ☑ 遵循以下良好保安守則：

□ 定期更新裝置，例如Wi-Fi路由器和網絡電視機頂盒的韌體及軟件

□ 避免使用Wi-Fi路由器的預設設定，如預設的服務設定識別碼(SSID)和管理員密碼

□ 採用穩固安全的通訊設定，例如使用AES 256位元加密的WPA2標準

□ 啓動Wi-Fi路由器的內置防火牆功能，以保護你的內部網絡

□ 如不使用，應把Wi-Fi路由器關閉

給學校和中小企的建議：

□ 制訂正確使用Wi-Fi網絡的政策，以及為使用者制訂資訊科技保安指引

□ 使用MAC位址過濾，或使用其他穩妥的機制進行使用者認證

□ 把Wi-Fi路由器及無線網絡接駁點妥善安裝在適當位置

□ 限制訪客專用的Wi-Fi網絡連接到內部網絡

□ 定期檢查日誌記錄，以偵測可疑活動

網絡安全資訊站
www.cybersecurity.hk

政府資訊科技總監辦公室