



我们的 20 个最常用的犯罪预防提示

保护身份文件



1. 为避免输入信用卡的详细信息，考虑使用第三方支付系统进行在线交易，例如 PayPal。专门为在线购物或海外旅行准备一张信用额度较低的信用卡。
2. 在线订阅或注册时，请勿使用真实的出生日期。出生日期可能是必填项，但并非法律要求。例如：使用 01/01/出生年份 – 确保您的年龄是真实的，但又不会暴露您的身份信息。
3. 在任何电子设备上使用强密码 – 使用复杂密码、图案密码或 PIN 码（由强到弱的顺序）。另外，也可考虑使用面部识别或指纹识别（均为强安全模式）。请注意最简便的方法往往不是最安全的。您的手机中可能存储了海量的敏感数据，考虑对账户使用“双重验证”。对于所有触摸屏设备，定时清洁屏幕来去除手印痕迹以免泄露密码信息。
4. 切勿向他人透露您的 PIN 信息。当心泄露通常在信用卡背面的 3 到 4 位的安全码 (CVV)。通过查看浏览器地址栏的安全信息，包括挂锁标记、绿色的前缀字体或路径前缀为“https”，来检查网站的支付安全。取消选中“在文件中保存所有付款信息 (Keep these payment details on file)”复选框。
5. 加密保存所有重要文件。考虑对您的设备进行安全加密。使用加密的即时通讯系统，例如 Signal。考虑使用虚拟专用网 (VPN)。一旦使用完 Wi-Fi 请立即清除网络连接记录。使用“匿名”模式，以防泄露浏览历史记录。
6. 请注意 Wi-Fi 安全，尤其是诸如婴儿监视器之类的物品安全。请确保为所有网络相关物品重新设置密码，特别是 Wi-Fi 设备、Internet 路由器、计算机、笔记本电脑、平板电脑、手机、电话留言机、智能电视等，请环顾您房间内的所有设施，确保所有 Internet 相关的物品的安全。
7. 请在所有网络连接设备（包括手机）上安装防火墙软件、防病毒和防恶意软件的系统。保持软件在最新的版本 - 考虑将设备设定自动更新。并确保您为任何设备都安装了最新的软件更新和补丁程序，因为这样可以消除漏洞的威胁。请一次只安装或使用一款防病毒软件并且只从官方网页下载程序。
8. 粉碎任何不需要的文件（银行对账单、帐户信息），特别是包含个人信息（例如签名、出生日期）的文件以及信用卡和会员卡。在当地的邻里照看互助团体 (Neighbourhood Watch group) 可能有碎纸机可以借用 - 请您询问当地犯罪预防官员 (Crime Prevention Officer, CPO)。对于一般信件，只需在丢弃回收之前，撕下您的姓名和地址。养成保留收据以及检查银行对账单的习惯。
9. 当您在车上留下任何有价值的设备时，不要只是放在隐蔽的地方，而应该关机从而避免让犯罪软件猜中您存放的地方。
10. 请在政府网站注册下列警报事项：www.staysmartonline.gov.au www.scamwatch.gov.au
www.esafety.gov.au/about-the-office/newsroom/cyberzine

FOR EMERGENCIES (Including anyone on your property)	000
TO REPORT ANYTHING SUSPICIOUS (Crime Stoppers)	1800 333 000
TO REPORT NON-EMERGENCY CRIME (Police Assistance Line)	131 444
IF YOU'RE NOT SURE (Hornsby Police Station)	9476 979
TTY—To ask for Police, type PPP	106
SPEAK AND LISTEN	1 800 555 727

11. 保持信箱安全，务必把锁锁在信箱上 – 请考虑使用“Tubular Pin Tumbler Lock”。定期清理信箱邮件，不要让邮箱的信件溢出。请明确重要文件何时送达，并调查迟缓送达的原因。
12. 不要将个人信息（例如出生日期、婚前姓名、签名）通过电话或上门、电子邮件或网络问卷调查等形式发给陌生人。请删除您车辆中的所有个人文件和信息。
13. 请检查您在社交媒体上的隐私和安全设置，以确保网络安全。
14. 电子设备使用完毕后，请务必使用清理软件删除所有个人信息。请对电子设备进行加密设置，然后重置成出厂设置。（出厂重置将删除加密密码）如果不再需要使用设备，请使用磁铁来销毁数字内存。如能使用锤子、钻子或剪刀则效果更好。
15. 切勿让浏览器记住您的密码。如果不知道如何设置，请寻求帮助 - 这非常重要。
16. 了解网络上的最佳预防犯罪讯息。邻里照看互助团体 (Neighbourhood Watch) 设立了网站 www.watchout.org.au，为您指出正确的方向。
17. 请注意，社交媒体可以设定上传照片，标识拍摄地点的「地理位置」信息，请考虑更改社交媒体设置，删除此设置。考虑是否避免在社交媒体上进行“签到”，避免让无关人士知道您去过哪里，或喜欢去哪里。
18. 在咖啡馆或餐厅时，千万不要让信用卡离开您的视线。考虑使用防无线识别系统 (Radio-frequency identification, RFID) 的袖子，钱包，或背包来保护信用卡和护照，以防信息泄露。如果可以，请直接到银行分行领取新信用卡。
19. 不要打开可疑文件、弹出窗口或电子邮件及其附件 – 请直接删除可疑文件。如果不确定，请通过电话簿或网络搜索等单独来源，去验证联系人等信息是否正确。
20. 如果您认为自己的身份已经被窃取，请迅速采取行动。请与下面的警察 (PAL) 和 iDcare 联系。为了保护他人，请举报所有涉嫌欺诈或欺诈行为 - 使用网站 www.scamwatch.gov.au/report-a-scam 中的“To Report a Scam”。对于网络犯罪，请向 Australian Cyber Security Centre ReportCyber (previously ACORN) cyber.gov.au/report 举报。请每年检查一次您的信用报告（如果不急于看报告，是免费的）。请访问网站 www.mycreditfile.com.au 尽早查看您的信用情况。

This information was compiled by volunteers with Neighbourhood Watch within Ku-ring-gai and Hornsby. Please contact your Crime Prevention Officer (CPO) at Hornsby Police Station for more information. Phone: 9476 9799.

Tips and other resources are available to download free from the Neighbourhood Watch in Ku-ring-gai & Hornsby website: au-NHWKuringgaiHornsby.org/Tips/.

See also the community's one-stop-shop of crime prevention information: WatchOut.org.au.

Follow us on [Facebook](#), [Twitter](#) or at our [website](#). Contact us at: NHWKuringgaiHornsby@gmail.com.