Neighbourhood Watch
Ku-ring-gai & Hornsby

Our 20 Favourite Crime Prevention Tips for

PROTECT YOUR IDENTITY

1. Your email is your MOST important online account, since password reset instructions from websites are sent to your email (or SMSed to your phone).
   - Protect your email with a strong, unique password, plus use two-step login.
   - Use two-step login (typically password plus SMS) on ALL important websites.
   - Use DIFFERENT, strong passwords on at least important websites, if not all websites.
   - Use password manager software or write your passwords in a diary.
2. Consider using a third-party payment system such as PayPal for Internet transactions, to avoid entering credit card details into websites. Consider having another credit card with a low credit limit to be used specifically for internet purchases, or for overseas.
3. Never share your card PIN. Beware sharing the 3-4 digit Card Verification Value (CVV), usually on the back of a credit card. Immediately sign new cards.
4. Check internet sites are secure for payment by looking on the address bar for the padlock symbol, green background colour, or the 's' in the 'https' prefix. Untick the box: 'Keep these payment details on file'. NEVER allow your browser to remember passwords.
5. Keep receipts and always check bank statements for fraudulent transactions.
6. NEVER let your credit card out of your sight in a café or restaurant – go with it! If possible, collect any new credit cards from the bank branch.
7. Consider using Radio-frequency identification (RFID) protection (sleeves, wallets, bags etc.) for credit cards and passports. Note: Legally you must report missing or stolen passports to the Australian Passport Information Service (APIS) on 131 232.
8. When registering on a website, use an email which does NOT look like your name.
9. Use a phantom date of birth when you subscribe or register online. It may be a compulsory field, however, it is NOT legally required. For example use 01/01/ followed by your year of birth - to keep your age demographic intact, but your identity safe.
10. Never give out personal details (e.g. date of birth, maiden name, signature) to unknown people, whether by phone, for surveys, at the door, by email or on the internet.
11. Set your browser in 'incognito' or 'private' mode, in order to stop websites tracking you.
12. Check your privacy and security settings on social media. Consider whether to avoid 'check-ins' to places on social media.
13. Photos can contain 'geotag' information that identifies the location where they were taken. Consider changing the settings to remove the geotag.

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 9799
TTY—To ask for Police, type PPP	106
SPEAK AND LISTEN	1 800 555 727

ENGLISH

14. Use a strong password on mobiles, tablets and laptops.
    - Use (in order of strength) complicated passwords, or a pattern, or a PIN.
    - Alternatively, consider using facial or fingerprint recognition (both strong). Note that the easiest (read 'laziest') method may not be the most secure - your devices can contain a HUGE amount of sensitive data about you, your home, your emails.
    - Set a NEW strong password on devices such as CCTV cameras, baby monitor, Internet router, telephone answering-machine, smart TV, smart speaker. Look around your home!
    - Download apps from only the official stores. Don't jailbreak your device.
    - Install the latest software updates and patches to your devices, as these help to stop viruses.
    - Also install firewall and anti-virus software on all devices, including your mobile phone. Set all updates to'Auto'.
    - Before disposing of a device, remember to delete all personal information. For laptops, use the Wipe Disk or Reset features of Windows. For tablets and mobiles, reset to factory settings. (The reset will delete the encryption code.) For external hard disks or USB sticks, use data erase software or destroy with a hammer or drill.
    - For all touch screen devices, regularly clean the screen to remove tell-tale marks.
15. Avoid using public hotspots (cafes, airports, hotels). Use mobile data instead. If you do use a public hotspot, get your device to 'forget' it once you are done.
16. Remove all personal documents from your vehicle. When leaving a device in a vehicle, don't just remove it from view, turn it off, to avoid a criminal detecting the device's Wi-Fi/mobile radio-waves.
17. Shred any unneeded documents (statements, accounts) that have your personal details (e.g. signature, birth date), as well as credit cards and loyalty cards. Your local Neighbourhood Watch group may have a shredder to borrow. For generic letters, simply tear out your name/address before recycling. Keep your maibox secure. Put a lock on your mailbox – consider a 'Tubular Pin Tumbler Lock'. Remove mail regularly. Don't allow your mailbox to overflow. Know when important documents are expected to arrive, and investigate if they are late.
18. Do not open suspicious texts, pop-up windows or emails/attachments – delete them. If unsure, verify the contact through an independent source such as a phone book or online search. Do not use contact details provided in the message sent to you.
19. Use:
    - https://haveibeenpwned.com. If it tells you that a website you use has been hacked, change your password for that website.
    - Check your credit report annually (FREE if not in a hurry) and as soon as you are concerned, at www.mycreditfile.com.au , Equifax, etc.
    - Sign up for the alerts from the government: www.staysmartonline.gov.au, www.scamwatch.gov.au, https://www.esafety.gov.au/about-us/subscribe.
    - Know the best crime prevention information on the internet. Neighbourhood Watch has created www.WatchOut.org.au to point you in the right direction.
20. If you think your identity has been compromised:
    - Act quickly and contact the Police (PAL). Contact iDcare.org FREE support contact@idcare.org 1300 432 273. Tell your bank or other institution, e.g. the ATO.
    - To help protect others, always report ALL suspected frauds/scams – use https://www.scamwatch.gov.au/report-a-scam or cyber.gov.au/report.

This information was compiled by volunteers with Neighbourhood Watch 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.