Neighbourhood Watch
Let's watch out for each other

eNews

Neighbourhood Watch
Ku-ring-gai and Hornsby
eNewsletter #579 - 15 November 2022

This weekly eNewsletter is compiled by Neighbourhood Watch volunteers as a service for residents in Ku-ring-gai and Hornsby council areas. The eNewsletter is a new type of Neighbourhood Watch; utilising the available technology to keep people more connected and up-to-date with local crime and safety issues.

The eNewsletter includes a selection of posts from our local police at the <u>Ku-ring-gai PAC Facebook page</u> (also known as 'eyewatch'), primarily for those not familiar with Facebook. We add anything interesting from a Neighbourhood Watch point-of-view - this could be a local newspaper article, a roadwork warning, crime prevention tip(s), an upcoming Neighbourhood Watch meeting, Q&As from residents, or an item from another Police command ("Crooks know no boundaries!").

🚗 Have you seen anything we should share with the community? <u>Please email</u> our NHW in Ku-ring-gai & Hornsby volunteers. We do value your contributions and thank you for your support.
🚗 Please feel free to share/forward this eNewsletter with your friends, family, colleagues and neighbours.
🚗 Reading our eNewsletter for the first time? <u>Click here to subscribe</u>.

---

15 November, from NSW Police Force: ⚠️ **MAKE THE SAFE DECISION** ⚠️

For all flood-related assistance, please contact the **NSW SES on 132 500**, or visit <u>nsw.gov.au/floods</u>.

Please save Triple Zero (000) for life-threatening emergencies only.

Those in flood affected areas are also urged to register their movements using the Register.Find.Reunite website – <u>register.redcross.org.au</u>.

---

13 November, from Australian Cyber Security Centre: ❗ **UPDATED ALERT** ❗

The ACSC has updated its advice regarding the Medibank cyber security incident

Remember, to be vigilant and monitor for any suspicious activity on your devices and accounts. Report unusual activity to cyber.gov.au, IDCARE (1800 595 160), and your bank.

Do not click on links in suspicious emails or messages that reference Medibank.

Report scams to <u>scamwatch.gov.au</u>.

For further guidance, visit <u>here</u>.

12 November, from Ku-ring-gai command: Thank you to everyone who stopped and had a chat with us yesterday at Bunnings Warehouse Australia, Pymble to celebrate Crime Prevention Week.
And thank you to our lovely Neighbourhood Watch Volunteers for attending. It was great to share stories with the local community and watch you all win some prizes on the wheel of fortune! 🎁

11 November, from NSW Police Force: Police are appealing for information from the public after a pedestrian was hit by a car that failed to stop at Bankstown yesterday.

Just after 11am (Wednesday 9 November 2022), a 71-year-old woman was standing next to her silver Mercedes which was parked in a designated parking space off the roadway on the eastern kerb of Highland Avenue. Police have been told the woman was then struck by an early 2000s model white Toyota Camry travelling south along Highland Avenue, throwing her to the ground. The car failed to stop and assist the injured pedestrian. The vehicle was last seen turning left into Marion Street. A witness rendered first aid before calling emergency services. The woman was treated at the scene by NSW Ambulance paramedics and taken to Liverpool Hospital for treatment of pelvic and abdominal injuries.

Officers from Bankstown Police Area Command attended and established a crime scene, which was forensically examined by police from the Metropolitan Crash Investigation Unit. Investigators are appealing for anyone with information about this incident, or had dashcam vision, is urged to contact **Crimestoppers on 1800 333 000** or nsw.crimestoppers.com.au**.** Information is treated in strict confidence.

10 November, from Neighbourhood Watch Australasia:

#QuickTip A steering wheel lock is still one of the best anti-theft devices around. If a car thief can't turn the steering wheel they can't drive, so they'll move on to an easier target. Simple.

---

09 November, from Ku-ring-gai command: Sextortion is a form of blackmail where someone threatens to share intimate personal images of you online unless their demands are met.
It is against the law. If this has happened or happens to you in the future, please contact NSW Police Force as we can help.
Remember, it is not your fault, you are not alone and you have not done anything wrong.

SEXTORTION

Sexual extortion (or sextortion) is a form of blackmail where someone threatens to share intimate personal images of you online unless their demands are met. These demands are typically for money, more intimate images or sexual favours.

NSW Police Force takes sexual extortion seriously and there are consequences.

In NSW the recording or capture, distribution, as well as the threat to record or distribute, an intimate image is against the law.

If you experience image-based abuse police can investigate.

Do not pay or send any more images or videos of yourself.

Stop all contact with the blackmailer

Notify the relevant social media platform

Secure your accounts.

Remember, it is not your fault, you are not alone and you have not done anything wrong.

15 November, from ID Support, NSW Government: Two new flyers from ID Support, NSW Government:
How to Protect your Identity and
We can Help if your Identity is Stolen.

If your identity is compromised, contact **ID Support, NSW Government on 1800 001 040**.

NSW
GOVERNMENT

How to protect **your identity**

'Having your identity stolen can be distressing. It can have serious financial costs, and can take hours of time calling different organisations to cancel and replace documents and credentials.

The effects of identity theft can be ongoing and highly stressful, and often customers are not aware they have been a victim of a crime until it is too late.

The NSW Government understands how important it is for customers to keep their personal information secure and we are working to ensure their identity is protected.

ID Support NSW supports customers whose NSW Government credentials have been compromised.'

– The Hon. Victor Michael Dominello, MP
Minister for Customer Service and Digital Government

About identity theft

Identity theft is when a criminal gains access to your personal information without your consent.

They can then run up debts in your name by fraudulently applying for phone contracts, credit cards or loans. Scammers can also make illegal purchases, gain access to your bank or email accounts, change your mailing address and more.

Whether it happens online, offline, or both, the damage can be serious. Identity theft can impact your personal finances. Until it's resolved, this can make it difficult for you to get loans, credit cards or a mortgage.

Around 1 in 4 Australians have been a victim of identity theft at some point in their lives. On average, they lose more than $4000.

How to prevent identity theft

Here are some simple steps you can take:

- Only take the ID you need when you go out and keep it in a secure place.
- Use a digital wallet for your payments and ID cards where possible.
- Lock your devices with a passcode, passphrase and/or biometric (such as fingerprint or facial recognition).
- Use long, complex passphrases by combining multiple words into a string that's easy for you to remember. It should contain a good mix of upper and lowercase letters, numbers and symbols, to make it harder to crack.
- Avoid using public Wi-Fi where possible and when needed use a Virtual Private Network (VPN).
- Secure your browser – visit cyber.gov.au for more information.
- Don't provide personal or financial information via social media, text or email.
- Set your social media profiles to private and limit the amount of information you share on them.
- Review the privacy policies of companies to understand how your data will be used, stored and protected, and ask what they do and don't need to keep.
- Use multi-factor authentication on digital services where it's available, such as getting a code sent to your phone by SMS before you can log in to your account.
- Don't click links or popups you didn't request or weren't expecting.
- Regularly review your bank statements and credit reports, and sign up for alerts with your banks and creditors to ensure early detection of any identity theft.
- Use a cross-cut shredder when destroying any documents with your personal info.

If your identity documents have been stolen or compromised, please contact ID Support NSW. You can call **1800 001 040**, or use our online form at **nsw.gov.au**

🔍 ID Support NSW

How to recover your identity

If you're a victim of identity theft, it can be hard to know where to start. But it's important to act quickly.

Follow these steps:

Notify your financial institutions

Report the breach as soon as possible. Request extra security measures for your accounts such as placing a block on your account, closing it or adding passwords and PINs.

You can also tell other money transferring institutions such as PayPal, Western Union and Gumtree about what happened.

Check your credit reports

Visit moneysmart.gov.au to check your free credit score and credit report.

This means you can see if there has been any unfamiliar activity in your name, including:

* credit applications you never made
* accounts you never opened
* enquiries you never made
* personal information you never provided.

The website also provides the contact details for the three main credit reporting agencies. You can contact them if you want to know more about your credit report or how to place a block on credit applications in your name.

Freeze your credit

Freezing your credit means that credit reporting agencies can't disclose your personal information to credit providers unless you give them your written consent, or they're required by law to do so. A ban also prevents accounts being opened in your name.

Submit a police report

Visit cyber.gov.au and submit a report. This will be assessed by the appropriate police jurisdiction. You'll need to provide personal information and details of what happened, including dates and relevant financial transactions.

After you submit your report, you'll receive a receipt with a unique Report Reference Number. You can provide this number to financial institutions or other organisations as proof that the breach has been reported to police. You may be contacted by police for more information.

Change and strengthen passwords

Change all your important passwords. Don't use obvious or identifying information like your date of birth. Use complex passphrases that are easy for you to remember but hard for hackers to crack. Make sure you include upper and lowercase letters, numbers and symbols. It's also important to use different passphrases for different accounts (email, banking, social media etc).

Establish multi-factor authentication

Multi-factor authentication (MFA) is a security measure that requires 2 or more security steps. MFA typically requires a combination of something you know (such as a password, PIN or secret question) and something you possess (such as an access code generated by an authenticator app, or a verification text or email). This reduces the risk of others accessing your account.

Replace your identity documents

If your NSW Government proof of identity documents or credentials are stolen or compromised, you may need to cancel and replace them. This can prevent your ID being fraudulently used.

If your identity documents have been stolen or compromised, please contact ID Support NSW. You can call 1800 001 040, or use our online form at nsw.gov.au

🔍 ID Support NSW

ID Support NSW

NSW GOVERNMENT

We can **help** if your identity is stolen

Each year more than 150,000 Australians are victims of identity crime. If your NSW Government proof of identity documents or credentials are stolen or fraudulently accessed, it can be hard to know where to start. That's why ID Support NSW is here to help.

What is identity crime?

Identity crime happens when a scammer gains access to your personal information without your consent. It can happen online, offline, or a combination of both. In most cases, identity crimes involve scammers stealing money by pretending to be someone else, like you.

Identity crime can impact your personal finances. Until the issue is resolved, this could make it difficult for you to get phone contracts, credit cards or a mortgage.

Around 1 in 4 Australians have been a victim of identity crime at some point in their lives.

How identity crime can happen

There are many ways for your identity to be compromised, including:

- phone calls
- text messages
- emails
- fake profiles
- and other communications.

Scammers often pretend to be from a charity, a bank, a service provider or even the government.

Once they have your personal information, they can then fraudulently apply for credit cards or loans in your name, make illegal purchases, gain access to your bank or email accounts, tax file number or superannuation, change your mailing address and more.

If you get a call or message claiming to be from a business or organisation and something doesn't feel right, contact them separately, using the details on their official website. You can ask them to confirm if the contact is legitimate.

Introducing ID Support NSW

The NSW Government established ID Support to help people learn more about and prevent identity crime. We can help you improve the security and safety of your personal information, and support you if any of your NSW Government proof of identity credentials have been compromised. These include:

- Driver licence
- Birth certificate
- MyServiceNSW Account
- Security licence
- Firearms licence
- Working with Children Check
- Seniors Card.

We will continue to expand our services to help with other types of compromised documents.

What we do

If your identity falls into the wrong hands, ID Support can provide advice on how to:

- recover the security of your identity
- protect your identity in the future
- find support, including counselling services.

Common scams

Scams are always evolving and becoming more sophisticated and convincing.

Scams are often delivered by:

- email – often asking you to click a link which will compromise your device. Be wary if it's an organisation you don't do business with. Check for poor spelling and grammar, strange or blurred logos, poor formatting.
- text messages – will often have a link which will access your device and your contacts. Many suggest urgency, or a common situation such as a parcel delivery (asking you to pay the delivery fee).
- phone calls – situations are often unrealistic, and may come from robots/auto-diallers. A common scam is that your credit card is about to be charged and you're being given a chance to opt out, then asking you to provide your card details.

Warning signs

- You stop receiving mail at your address, especially bills and statements.
- You can't log in to your online accounts.
- You receive bills, invoices, or receipts for goods or services you didn't request.
- Your passwords appear to change without your permission.
- Bank or credit card statements include items you don't recognise.
- Devices or online accounts are accessed by third parties.
- Accounts show overseas transactions that you didn't make.
- Your superannuation balance is much lower than expected.

How to protect your identity online:

- Don't open unusual or unexpected texts or emails.
- Hover over links and if you don't recognise it, or if it looks suspicious – don't click on it.
- Don't give your details to unknown websites or websites you don't trust.
- If you're asked to provide your credentials, take action through the official website and not through unknown links.
- Choose strong unique passwords for all your accounts and change them regularly.
- Use complex passphrases that are easy to remember but also contain upper and lowercase letters, numbers and symbols so they're hard to crack.
- Add multi-factor authentication on accounts.
- Be curious about your information being collected by organisations.
- Remember that you have a right to know and ask how your information is used.

How to protect your identity offline:

- Secure your personal credentials at home and when travelling, don't write any credentials down on paper.
- Put a lock on your mailbox and securely destroy any documents you don't need if they have personal information.
- Be cautious about requests for your personal information over the phone and in person.
- Never give out personal information over the phone, especially if the caller is unknown or asking for payment.
- Order a free annual copy of your credit report from a credit reporting agency.
- Regularly check your bank and superannuation statements.
- Be curious about your information being collected by organisations.
- Remember that you have a right to know and ask how your information is used.
- If you receive a call requesting information or credentials, finish the call and call the service back using their official and publicly listed phone number.

Be cautious about requests for your personal information over the phone and in person.

Get in touch
We have a dedicated support team who provide advice and solutions for your compromised NSW Government identity credentials.

Call us on 1800 001 040
Monday to Friday, 9am to 5pm

To find out more visit nsw.gov.au

🔍 ID Support NSW

Your identity is important. Let's protect it.

Email NHW here for the pdfs of either of the above flyers in your inbox.

Neighbourhood Watch (NHW) Week/Coffee with a Cop @ Bunnings, Pymble
We held a successful joint NSWPF/NHW Crime Prevention stall with goodies last Friday 11 November. Thank you to Bunnings for the invitation. Thank you to Graham, Kerrie and Mick for their help on the day.

One question from a resident was how to secure an expensive trailer.
Our response: Try wheel chocks chained to the wheels. Maybe a camera, and a very visible sign adjacent to the trailer, with a warning that you are on camera? (This kind of sign can be bought at your local hardware store.) There are also many types of tracking product on the market, such as AirTags, which won't stop your trailer being stolen, but may help you recover it.

Note: NHW cannot endorse any product or service - you must do your own research.

---

15 November, Shared with permission from the Thornleigh, Westleigh and Normanhurst Community (AU) :
What's the deal with people helping themselves to flowers from your driveway garden? Including possibly neighbors? Is that legally allowed?
Just to clarify, this wasn't done by an animal, someone had used scissors or secateurs and

clean cut 3 flowers from three different plants at the stem. I don't mind people taking flowers, they'll grow back I'm sure. It'd be nice if they'd asked first.

---

15 November, from Neighbourhood Watch NSW: Vote for Neighbourhood Watch NSW Inc to share in $500,000 in grants from MyGiving Circle

Neighbourhood Watch NSW acts as a conduit between the Police and communities. We are a vibrant, inclusive and effective organisation that improves the safety, security and connection of community life across New South Wales. We do this by supporting our members and partners in promoting crime prevention, education, resilient communities and social inclusion.

This grants round closes December 30th and MyGivingCircle will give $90,000 to #60 charities, including #10 grants for Oz Community charities. Vote here.

---

13 November, from NSW Health: NSW is currently experiencing a new wave of COVID-19, with positive cases and hospital admissions increasing across the state.
While mask wearing is no longer mandatory in NSW, it's a little thing we can all do to protect each other from COVID-19 circulating in the community. Pop on a mask when indoors or in crowded places, such as on public transport or at social and sporting events. Pack some spare masks in your bag for friends and family. You never know who is vulnerable to COVID-19 around you, and wearing a mask gives you extra protection too. Together, let's stay COVID safe this wave.

For further advice on keeping COVID safe, visit nsw.gov.au/covid-19/stay-safe

Wearing a mask in crowded places.
Little things. Big difference.

NSW GOVERNMENT

---

13 November, from Hornsby Shire Council: SOFT PLASTICS ♻️✨ | Have you been recycling your soft plastics at a supermarket?
As you may have read in the news, a large soft plastics recycling program collecting plastics at supermarkets, has recently ceased operating. We are happy to share that our soft plastics recycling program is unaffected and still running. All soft plastics dropped at our Thornleigh Community Recycling Centre are sent to our partner, Plasmar - based in south-west Sydney - where they are sorted, shredded and re-formed into new products including fence posts, bollards, boarding and car park stocks. We are also actively looking at means to bring these recycled products back to our community to help create a strong circular economy in Hornsby Shire ♻️💪

👉 You can find more information about the Community Recycling Centre, here: hornsby.nsw.gov.au/crc�

---

12 November, Shared with permission from the Berowra Community group:
Unfortunately this backpack fell out of my pram while I was walking today. Has anyone seen this or picked it up?

---

10 November, from Neighbourhood Watch NSW: Слава Україні!
@ZelenskyyUa Neighbourhood Watch (NHW) New South Wales Australia recognises the ultimate NHW volunteer! Prevents the entire Neighbourhood from being stolen.

---

10 November, From today's Australian Cyber Security Centre (ACSC) newsletter alert: High Alert - Act Quickly
09 November 2022
Dear ACSC Alert Service subscriber
Update on the Medibank Private Cyber Security Incident

On Wednesday 9 November, Medibank Private advised that a criminal has released files on a dark web forum containing customer data that is believed to have been stolen from Medibank's systems. This data includes personal data such as names, addresses, dates of birth, phone numbers, email addresses, Medicare numbers for AHM customers (not expiry dates), in some cases passport numbers for international students (not expiry dates), and some health claims data. This remains under investigation by the Australian Federal Police. It's important that you:

- Remain vigilant and monitor all your devices and accounts for unusual activity. Report unusual activity to ReportCyber: cyber.gov.au/acsc/report
- IDCARE: idcare.org/optus-db-response
  (1800 595 160), and your bank.
- Be alert for scams that make reference to Medibank Private. Do not click on links in suspicious emails or messages that reference Medibank Private. Visit ScamWatch for help: scamwatch.gov.au/.

The ACSC has advice on practical ways to protect yourself online: cyber.gov.au/learn
You can follow these simple steps to boost your cyber security:

- Update your device: cyber.gov.au/updates and turn on automatic updates to ensure you always have the latest security protection.
- Turn on multi-factor authentication: cyber.gov.au/mfa to increase the security of your accounts.
- Set up and perform regular backups: cyber.gov.au/backups to copy and store critical information.
- Implement access controls to limit user access to only what is needed on devices.
- Stay up to date on cyber security threats and trends with ACSC Alert Service: medibank.com.au/health-insurance/info/cyber-security/.

If you think you may be affected by the Medibank Private cyber security incident:medibank.com.au/health.../info/cyber-security/, AHM customers should contact **13 42 46** and for Medibank Private customers **13 23 31**. Contact Medibank: medibank.com.au/contact-us/
If you believe your Medicare card has been exposed, you can replace it at no cost through MyGov: my.gov.au/
The following websites can help you protect yourself and stay informed:

- Identity theft | Moneysmart moneysmart.gov.au/banking/identity-theft
- Identity fraud | OAIC: oaic.gov.au/privacy/data-breaches/identity-fraud
- Services Australia fact sheet: servicesaustralia.gov.au/what-to-do-if-youve-been-affected-recent-medibank-private-and-ahm-data-breach?

Read this alert on our website: cyber.gov.au/acsc/view-all-content/alerts/medibank-private-cyber-security-incident

Are you a victim of cybercrime? Visit ReportCyber: cyber.gov.au/acsc/report to take your next steps.

We use hyperlinks to give you more information. If you don't want to click hyperlinks, you can search for the information on our website.

CONTACT US

Facebook: facebook.com/cybergovau

Twitter: twitter.com/CyberGovAU

Web: cyber.gov.au

Dates for the Diary

Thursday 17 November: Ku-ring-gai Council Workshop for Supervisors of Learner Drivers webinar 6:30-8pm. Bookings **9424 0843** and here.

Wednesday 30 November: Walk the Talk. PCYC Waitara return. 8:45-10:45am. Info

Wednesday 30 November: 7pm NHW Gordon/Killara/East Killara/part Pymble/part St Ives AGM @ St John's Anglican Church, Gordon. NHW Crime Prevention stall. All residents welcome!

From NHW in Ku-ring-gai & Hornsby: 'Our 20 Favourite Crime Prevention Tips for Apartments'

Tip #15: When moving in, consider installing new locks. You don't know if the unit has been burgled before. For extra security it's a good idea to get locks changed and re-keyed. This includes the mailbox. Request our 20 Tips for MAILBOXES.

Tip #16: Request your Body Corporate pursue Crime Prevention initiatives, eg: 'Rapid Removal' graffiti policy, monitored CCTV, landscaping to reduce the opportunity for crime, secure fences & gates, security lighting.

Tip #17: Do not leave your car park remote control or any valuables on view in your vehicle, even if it is locked and in the secure parking area.

Tip #18: Consider replacing the main door lock(s) with high-quality deadlocks. Replace any screws with longer ones to secure any doorchain/doorbar.

For more tips and translations, look at our website 'Tips' page here. Or try our WatchOut! website here, for links to some great information available on the internet. Or request a copy

in your inbox <u>here</u>.

Isle of Wight Police
16 hours ago

Footwear review for those wishing to run from C Shift.

'Nike Vapour Air Max Plus' - This trainer provides good cushioning for the initial sprint when requested to stop by Police. After several hundred meters and as the run develops their lack of support shines through, meaning you end up in cuffs. As a result we'd score this trainer a 4/10 for those wishing to run 😜

Result - One male in Sandown arrested and in custody for possession with intent to supply. We have seized three large bags of cannabis, over £1000 cash and a vehicle. A second male from Sandown has also been arrested in connection with this offence.

I wonder what trainer we will be reviewing next 😲

Enquires are on-going.

Sgt Winchester

👍 645   💬 131   ↗ 102

Posted in r/CasualUK reddit

IMPORTANT CONTACTS & LINKS

Emergency (Police/Fire/Ambulance): **000**
TTY: 106

NSW Police - Ku-ring-gai Police Area Command (PAC): **9476 9799**
Hornsby Police Station, 292 Peats Ferry Road, Hornsby 2077

Local Police Facebook page: @Kuring Gai PAC
Non-emergency two-way communication

Police Assistance Line (PAL): 131 444
For non-urgent minor crime.

NSW Police Community Portal
Online reporting of non-emergency minor crime: lost property, intentional damage, graffiti or theft.

Interpreting & Translating Services: 131 450

NSW Police - website for crime prevention advice
Never be afraid or embarrassed to report a crime, concern or fear you have to the Police. The Police are here to help you.

Crime Stoppers NSW: 1800 333 000
Report crime anonymously
Report suspicious activity ASAP

Neighbourhood Watch within Ku-ring-gai and Hornsby:
Website au-NHWKuringgaiHornsby.org
Facebook @NHWKuringgaiHornsby
Facebook Group NHWKuringgaiHornsby
Twitter @NHWKRGHornsby
Email NHWKuringgaiHornsby@gmail.com

WatchOut!

WatchOut! - the NHW NSW one-stop-shop for crime prevention links:
Website WatchOut.org.au
Facebook @NHWWatchOut

Local Facebook pages/groups:
Neighbourhood Watch - Berowra
Brooklyn Neighbourhood Watch
Neighbourhood Watch - East Killara
Neighbourhood Watch - Galston, Glenorie, Arcadia, Dural (Rural Areas)
NHW Galston, Glenorie, Arcadia & Dural (Rural Areas) Facebook Group
Neighbourhood Watch - Gordon
Neighbourhood Watch - Hornsby
Neighbourhood Watch - Killara
Neighbourhood Watch - Mt Colah
Neighbourhood Watch - Mt Kuring-gai
Neighbourhood Watch - Normanhurst
Neighbourhood Watch - Pennant Hills
Neighbourhood Watch - St Ives
Neighbourhood Watch - Thornleigh
Neighbourhood Watch - Turramurra
Neighbourhood Watch - Wahroonga
Neighbourhood Watch - Warrawee

Face-to-Face/printed newsletter groups:
Neighbourhood Watch - East Killara
Neighbourhood Watch - Gordon (part)/Killara (part)/Pymble (part)
Neighbourhood Watch - Hornsby (Jubilee St)
Neighbourhood Watch - Mt Colah
Neighbourhood Watch - St Ives (Lynbara Ave)
Neighbourhood Watch - Turramurra (The Chase)