Neighbourhood Watch
Ku-ring-gai & Hornsby

Our 20 Favourite Crime Prevention Tips for

Cryptocurrency

The cryptocurrency world is unfortunately rife with scammers. Everyone who reaches out to you with an investment opportunity via phone, email or messaging applications will be a scammer who hopes to lure you into sending them your crypto with promises of large returns. There are also many automated scams that lure you into claiming free tokens, but actually drain your crypto wallet. Never give anyone your seed phrase (typically 12 or 24 words) as they will steal your crypto. Assume everyone is a scammer!

1. Use only reputable cryptocurrency exchanges with strong security measures. Make sure the company or website is not named on the government's moneysmart.gov.au/check-and-report-scams/investor-alert-list or on the International Organization of Securities Commissions (IOSCO) investor alerts portal, which has warnings from overseas regulators.
2. Only use trusted sources for news and information regarding cryptocurrencies. Ensure the person trying to sell you a financial or investment product, or who is giving you financial advice, has an Australian Financial Services (AFS) license.
3. Always enable 2 Factor Authentication on your accounts when dealing with a cryptocurrency exchange website. This adds an extra layer of security. Create strong, unique passwords for each of your accounts and change them regularly. Check your accounts regularly for any unauthorized activity. For long-term crypto currency holdings, consider using cold-storage solutions that are completely offline.
4. Beware of fake crypto wallets - Pay attention to the design, functionality, and usability of the wallet. Look for any red flags, such as unusual prompts or requests for sensitive information, lack of options to set up two-factor authentication (2FA), biometric authentication, and hardware wallet integration. Be alert to strange tokens appearing in your digital wallet that you did not trade yourself.
5. Beware of fake crypto exchanges – Look for signs like: unregistered with AUSTRAC (Australian Transaction Reports and Analysis Centre) and lack of clear information about the company and team. Search the internet for the exchange name with the word 'scam', 'review' or 'warning'.
6. Tokens can easily be created with any name, including well-known currencies. Identify a fake token by comparing its contract address with the official one listed on the legitimate token's website or official communications. Use official token lists – avoid using links from unverified sources. Check creation date, transaction history, and the number of coins in circulation – a newly created token with minimal history is a red flag.
7. Store your cryptocurrencies in hardware wallets rather than online or on exchanges. Update your wallet software regularly and any other security software you use. Backup your wallet regularly and store backups in multiple secure locations. Beware of requests to send crypto directly to personal wallets instead of using the platform's official wallet.
8. Avoid public Wi-Fi for transactions; Use a private Wi-Fi network to connect to your crypto account or wallet. Scammers can intercept information sent over public Wi-Fi.
9. Encrypt sensitive files and data related to your cryptocurrency activities.

FOR EMERGENCIES (Including anyone on your property)	000
TO REPORT ANYTHING SUSPICIOUS (Crime Stoppers)	1800 333 000
POLICE TO ATTEND NON-URGENTLY WITHOUT LIGHTS & SIRENS (Police Assistance Line)	131 444
IF YOU'RE NOT SURE (Hornsby Police Station)	9476 9799
POLICE COMMUNITY PORTAL (Minor crime – no emergency/investigation)	portal.police.nsw.gov.au
TTY—To ask for Police, type PPP	106
SPEAK AND LISTEN	1 800 555 727

ENGLISH

10. Be wary of phishing scams and never click on suspicious links or provide personal information. Stay informed about the latest threats and best practices in cryptocurrency security.
11. Always stop and check before you act. The scammers will often pressure you to act quickly. Don't let them rush you into a bad decision. Double-check all transaction details before confirming in order to avoid mistakes.
12. Be cautious of too-good-to-be-true investment opportunities and do thorough research. Read websites carefully**.** Verify listed addresses or phone numbers. Look for broken links, spelling mistakes or bad grammar. Be wary of a promise of large instant rewards if you sign up now, or large returns over a short period of time. Avoid crypto service providers that withhold investment earnings for 'tax purposes'.
13. Beware of requests for payment in crypto. It is very unlikely that any legitimate financial services firm will ask you to pay exclusively in crypto. Be wary of any recruiter, online romantic partner, or online acquaintance who asks for a crypto payment.
14. Scammers sometimes get you to install custom crypto broking software to supposedly track your crypto holdings. If you do, it could infect your computer with viruses and other malicious code. The scammer may be able to search your computer for personal details, steal your ID, and access your finances.
15. Scammers use cryptocurrencies, like Bitcoin or Ethereum, because they are not easily recovered. Crypto can be sent overseas quickly with limited oversight. Be aware that crypto is technically complex, but in some ways it's like a form of digital cash. Once it has been spent or transferred, it's impossible to retrieve, which scammers like. (Also be aware that the value can go up or down quickly and there are no guaranteed returns.)
16. Avoid sharing details about your cryptocurrency holdings publicly or with untrusted parties.
17. If you think you have been interacting with a crypto scammer, and have paid them money, contact your bank and other important services and let them know. You can ask for the fraud department, which will guide you through steps to secure your finances and other information.
18. If you think you have been scammed, it's important to change the password or passcode you use to access the computer, your main email password, and the master password of your password manager, if you use one.
19. Report any scam on the Scamwatch web site at **scamwatch.gov.au/report-a-scam**. This will help the Australian Competition & Consumer Commission (ACCC) investigate this scam and others like it, and allow them to issue warnings to others. Crypto scams are new and any information you give will be very valuable in helping limit the activities of these scammers. You can also report any online scam as a Cybercrime to the police via the Australian government's ReportCyber website at cyber.gov.au/acsc/report.
20. Check the following websites for further information about scammer's tactics, etc:
    moneysmart.gov.au/financial-scams/investment-scams
    scamwatch.gov.au/types-of-scams/investment-scams
    beconnected.esafety.gov.au/topic-library/identifying-and-avoiding-scams/crypto-scams/what-is-a-crypto-scam
    beconnected.esafety.gov.au/topic-library/identifying-and-avoiding-scams/crypto-scams/report-crypto-scams-and-update-your-details
    austrac.gov.au/business/your-industry/digital-currency-cryptocurrency

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, X or at our website. Contact us at: NHWKuringgaiHornsby@gmail.com.

Jan 2025 V1 Crypto **ENGLISH**