Neighbourhood Watch SA

PANORAMA 1
NHW AREA 64
ANNUAL GENERAL MEETING
Trinity Church Hall, Pasadena

Monday 7.30pm
7th December

All interested residents are welcome to join our meeting and nominate for a Committee position at the AGM.
Our Christmas break up follows the meeting. Bring a plate and enjoy a drink and a snack with other volunteers.

Area Co-ordinator
Seshadri Vydyam
Ph: 0403486065
Email: vvsesh@gmail.com

YOUR ZONE REP

_____

Ph: _____

Reporting Graffiti
Council owned property
City of Mitcham 8372 8888
Stobie poles or ETSA boxes
ETSA Utilities 8404 5673
Private property 131 444
Offence in progress *Dial 000*

HOME AND BUSINESS FIRE PREVENTION

Fires caused by deliberate, reckless or negligent behaviour not only destroy communities and properties but have the potential to kill. South Australia Police is committed to identifying and apprehending people who deliberately light fires or engage in reckless or negligent fire lighting behaviour.

To help keep your property safe from fire, consider implementing these crime prevention tips:

• Lock your property and vehicle at all times.

• Keep rubbish bins in a secure area and remove rubbish regularly.

• Secure all combustible materials and flammable fuels away from your property.

• External doors should have minimal gaps to prevent papers and flammable items being pushed inside the property.

• Maintain vegetation around your property and remove plant debris.

• Maintain fencing and install external security lighting.

• Conduct regular inspections outside your property. Repair damage to fences and remove graffiti regularly.

• Join your local Neighbourhood Watch or Business Watch program to help keep the community safe.

For further information contact your local police station or visit www.police.sa.gov.au

If you see anything suspicious immediately call the Police Assistance line on 131 444.

If you have any information about who is deliberately lighting fires or engaging in reckless or negligent fire lighting behaviour call Crime Stoppers on 1800 333 000.

COVID-19
TRUSTED SOURCES OF INFO

Check your symptoms
healthdirect.gov.au

National updates
health.gov.au

Local updates and information
sahealth.sa.gov.au/COVID2019

The latest travel advice
smartraveller.gov.au

For general questions
Coronavirus Health Information Line: 1800 020 080

Work from home revolution during pandemic powers spike in cybercrime

By Daniel Ziffer, ABC Business, 30 October

Our work from home revolution has powered a spike in cybercrime, costing consumers more for everyday products and dragging billions of dollars out of the economy.

"The attackers have taken advantage of the situation," said Nicola Nicol, partner at consulting firm Pricewaterhouse Coopers (PwC).

"Attackers have started to look to take advantage of employees who are working from home and perhaps not thinking about security in the same way they would do in an office environment."

Breaches cost companies an estimated $7.6 billion in the last financial year as COVID-19 forced employees out of skyscraper towers, suburban offices and factories. And experts expect the eye-watering impact to rise.

The months between April and June saw a 65 per cent increase in cybersecurity incidents, according to PwC's 2021 Global Digital Trust Insights survey of thousands of business, technology and security executives from large companies.

Workers swap secure servers & buildings for kitchen tables

An astonishing number of employees moved quickly this year from working on computers linked to secure servers, inside buildings protected by pass cards and gates, to performing vital business roles from their kitchens and bedrooms.

That shift was always going to be an opening for malicious and opportunistic cybercriminals, according to University of Melbourne senior lecturer in computing and information systems Suelette Dreyfus.

"You've got many more 'BYO devices', home devices, little Angus who's 15 years old who's been on that device playing games that he's downloaded from the internet — and God knows what else.

You have problems — people using their wifi from home maybe they haven't updated the firmware on their wi-fi devices for five years - that's a security risk," Dr Dreyfus said.

More than half of malicious attacks are by financially motivated-criminals

In the past year, ransomware attacks have crippled organisation and institutions as varied as Victorian country hospitals, logistics company Toll, Service NSW, Anglicare Sydney, money management company MyBudget and the hot strip mill of BlueScope Steel's Port Kembla plant.

Attacks even shut wool sales across Australia in February.

Ransomware is malicious software that goes inside existing computer networks. Once in, it steals information from your computer and demands a fee for it to be returned or stops the system from working until a ransom is paid.

Ransomware attacks and state-sponsored attempts to harm critical infrastructure are also considered 'likely', said Nicola Nicol.

What you can do to make yourself cyber-safe

The good news is that the surveyed organisations expect to spend more money and pay more attention to the problem. The better news is that it is cheap, often free, to better protect your business and personal accounts.

Dr Dreyfus suggests some simple steps:

- Have 'full disc encryption' (FDE) turned on
- Always have a passcode on your phone
- Use two-factor authentication. For example, requiring a text message to your phone to get access to social media accounts on your computer
- Get password manager software
- Update your software regularly

"And don't reuse passwords, that's a bad idea," she said.

SA Police issue scam warning after fraudster impersonating NBN calls cybercrime unit

By Charles Brice, ABC News, 5 November 2020

South Australian police have issued a warning about a new scam targeting Adelaide locals, after the force's own cybercrime unit was among the recipients of one of the deceptive phone calls.

SA Police said scammers were ringing Adelaide landlines, advising recipients that their computers had been hacked and directing them to a website imitating the National Broadband Network (NBN).

"There is an NBN scam currently cycling through Adelaide landline numbers, and the Financial and Cybercrime Investigation Branch (FCIB), who investigate such scams, were one of the numbers to receive a call," police said in a statement.

To better understand the fraudulent operation, a member of the FCIB using secure software followed the caller's instructions and was led to a "poorly designed" website.

"The obvious indicator that this website is not affiliated with the NBN is that the text preceding the '.com' is weebly — a webhosting site," police said.

The officer was then told to carry out steps which resulted in remote access software being downloaded.

"The caller tried to reassure us that the software would help fix our internet problem," police said.

"We informed the caller that we couldn't open the program, so he had us click on [other] buttons, which attempted to download further executable programs.

"After we kept experiencing problems, the caller terminated the call."

Police suspect the scammer was attempting to gain access to personal information, including passwords for online banking.

They urged the public not to engage with scammers, and said the incident demonstrated that "no-one is safe from receiving scam robocalls, not even the police".

"Our advice to the community is to not download software that you are not familiar with, and never at the direction of someone over the phone," police said.

"If you receive a call and cannot be certain who you are speaking to, hang up the phone and call the organisation back on a known, reputable number."

Police Incidents   August - November 2020
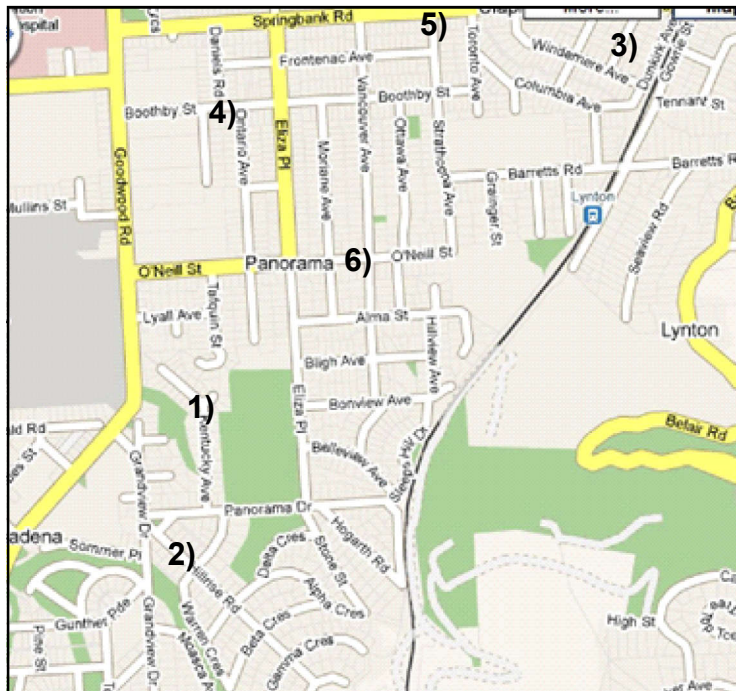
Date   Location   Details

PROPERTY DAMAGE

1. 18/08/20   Kentucky Ave   Graffiti marked on side fence.

2. 31/10/20   Hillrise Ave   Pipes and newly rendered walls damaged. Value $900.

THEFT

3. 1/9/20   Alberta Ave   2 loading ramps stolen from front yard. Value $1500.

4. 6/8/20   Boothby St   Secure unit block foyer entered by drilling lock. Unsuccessful attempt then made to drill lock into residential unit. Nil entry. $200 damage.

TRESPASS/BREAK-IN

5. 24/08/20   Springbank Rd   Entry gained to vacant property by smashing side window. Premises rummaged. Nil stolen.

6. 23/10/20   O'Neil St   Entry gained to property by forcing window. Cash and computer equipment stolen while occupants on holidays. Value $600.