Neighbourhood Watch SA

MARCH 2024   Quarterly Neighbourhood Newsletter of Panorama NHW Area 64/193

PANORAMA
NHW AREA 64/193

NEXT MEETING
Trinity Church Hall, Pasadena

**Monday 7pm
4th March 2024**

ALL WELCOME

Bringing local residents & police together for a safe & connected community

Area Co-ordinator
Seshadri Vydyam
Ph: 0403486065

Panoramaneighbourhoodwatch
@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*

How scammers use phishing attacks to get their way into your savings
ABC 17 August 2023

A message from an unrecognised email address or phone number. An urgent call to action. A suspicious-looking web link. A landing page where personal details must be entered.

Tens of millions of dollars are lost to phishing scams each year, and authorities say that figure is only increasing.

The scam may be an email or text message that appears to be from an official company or organisation, like the Australian Tax Office or Netflix.

Victims will be urged to act quickly to fix a problem with their account, or reconfirm their contact details, being directed to a page that looks remarkably similar to one used by the company.

The fake webpages will require victims to enter personal information such as bank account details or email passwords.

This information is then used to access bank accounts, where the scammer can transfer money to themselves at will.

The phishing frenzy in Australia

The latest figures reveal phishing is a practice that is only becoming more and more widespread.

Phishing was the most reported scam to Scamwatch in 2022, with the government website recording 74,573 complaints — a 4.6 per cent increase on the previous year.

In 2022, the total financial losses from phishing reported to Scamwatch and the Australian Financial Crimes Exchange totalled $157.6 million.

But despite the widespread financial toll on Australians, scams remain significantly under-reported nationally.

According to the Australian Competition and Consumer Commission, just 13 per cent of scam losses are reported to Scamwatch, while roughly a third are not reported to any organisations at all.
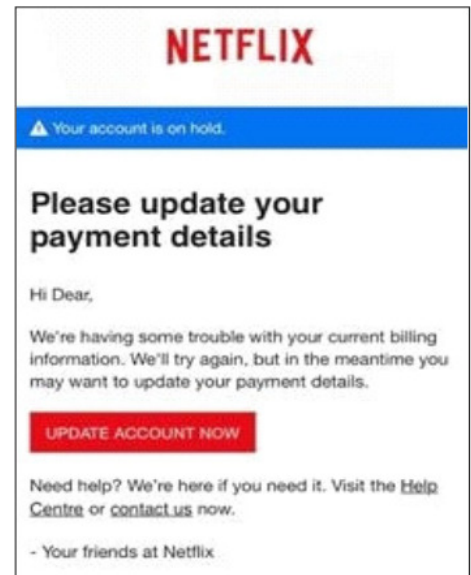
The Consumer Action Law Centre, says the organisation regularly encounters customers who are reluctant to report their losses due to shame and embarrassment.

Nearly 20 per cent of reported phishing scam attempts last year were bank impersonations, with more than $20 million lost.

What you can do after you've been phished

Recourse can be difficult to obtain for phishing victims.

Banks have their own individual policies for dealing with cybercrime, and despite Australians losing a record $3.1 billion to scams last year, the big banks only compensated customers about $21 million.

Victims who are unhappy with how a bank has responded to their situation can complain to the Australian Financial Complaints Authority.

Australians who believe they've been phished are strongly encouraged to secure their personal information through IDCARE.

Russian man identified as Medibank hacker, hit with sanctions by Australian government

By Tom Crowley, ABC News 23 January 2024

The Australian government has announced sanctions against Russian man Aleksandr Ermakov over his role in the Medibank Private data breach.

It is the first time the government has used its cyber sanctions framework, which was legislated in 2021 to apply financial punishments to people involved in significant cyber attacks.

The personal information of 9.7 million Medibank customers, including names, dates of birth, Medicare numbers and sensitive private health information, was stolen in 2022. Much of it was published on the dark web.

The government said the Australian Signals Directorate and the Australian Federal Police had identified Ermakov as responsible for the attack.

The sanctions make it a criminal offence to provide the man with any assets, including cryptocurrency and any money through ransom payments, punishable by up to 10 years in prison.

"This is a very important day for cybersecurity in our country," Home Affairs Minister Claire O'Neil said.

"Medibank, in my view, was the single most devastating cyber attack we have experienced as a nation.

"We all went through it. Literally millions of people having personal data about themselves, their family members, taken from them and cruelly placed online for others to see.

"These people are cowards and they're scumbags. They hide behind technolog... The Australian government is saying that when we put our minds to it, we'll unveil who you are and we'll make sure you're accountable."

Authorities are pursuing additional leads in relation to the Medibank attack.

Ms O'Neil said authorities were focused on "a number of Russian cyber gangs" threatening Australia and working in coordination with cyber authorities in the US and UK.

A spokesperson from Medibank thanked the government for identifying Ermakov and putting sanctions in place.

Foreign Minister Penny Wong also announced the government had imposed counter-terrorism sanctions against 12 people and three entities linked to Hamas, Hezbollah, and Palestinian Islamic jihad.

Jonathan's bank transactions show exactly where scammers used his details - it sent him down a spiral of confusion and stress for weeks

By Widia Jalal, *ABC News* 9 January 2024

Horticulturalist Jonathan Garner is always on the lookout for deliveries.

A text message from an unknown number said Mr Garner's parcel delivery had been unsuccessful and prompted him to update his information to resume the delivery.

Desperate to get a hold of his parcel, he clicked on the link in the message and was greeted with a page sporting a logo and brand colours identical to Australia Post.

The layout of the page, as well as the icons and symbols, all looked familiar to him so he skimmed to the end.

The page displayed his shipment details, along with a tracking number and a section for his card details.

It turns out the message had directed him to a fake Australia Post website, and he had unknowingly given scammers access to his bank account by filling out the six-digit authentication code.

Multiple identical transactions to a local business

Later that same day, six transactions were made resulting in a loss of about $2,700 across multiple identical transactions to a local tobacconist – all using his bank account details.

Mr Garner spotted the transactions a few days later on his account and immediately contacted his bank to alert them and seek compensation.

He said the fraud team at Commonwealth Bank explained he had fallen for a phishing scam and said he was ineligible for compensation because he had authorised the transactions.

After several rounds of intense negotiation, he said he ended up recovering 75 per cent of his losses from the bank which told him to report the case to the police.

Advice from Australia Post:

Australia Post is aware of such phishing scams circulating and has urged people to take these steps to protect themselves.

• Report any suspicious message – whether on text, email or social media – from senders posing as the courier to scams@auspost.com.au

---

How can you report phishing scams to authorities?

If you've fallen victim to a scam, here are the steps to take – depending on your circumstances.

• Contact your bank or financial institution immediately if you have lost money

• You can also report to police via ReportCyber

• Be aware of other scams which may occur after a loss of personal information

• Contact IDCARE on 1800 595 160 if you have provided scammers with your personal identifying information such as drivers licence or passport

• Report scams to Scamwatch

ReportCyber is a national policing initiative which ensures your report will be referred to the right law enforcement agencies.

You may also want to note the unique report reference number to provide to other organisations.

Run by National Anti-Scam Centre, Scamwatch collect reports about scams to help warn others and to take action to stop scams.

Visit your local police station or call the Police Assistance Line on 131 444.

If you are unable to report the scam to ReportCyber, you can lodge a report at your local police station as an alternative.

Join as a NHW SA volunteer now!

NHW SA has plenty of volunteer opportunities, whether you're looking to volunteer regularly, or only once a year, there's something to suit everyone.

You could just turn up to our next meeting, you could become a supporter (enabling you to help with the delivery of these newsletters), or you could become a registered police volunteer.

Let us know if you'd like to join and we can help you get your registration started. Find out more on the NHW SA website: www.police.sa.gov.au/nhw/home/get-involved

Benefits of joining as a NHW SA volunteer

Joining can benefit your local community and provide you with many valuable opportunities.

Whether you want to be a leader for change, develop new skills or simply get to know your neighbours.

There are different volunteer options you can do, each with different benefits.

Find out more on the NHW SA website: www.police.sa.gov.au/nhw/home/why-join.

WHAT IS NEIGHBOURHOOD WATCHSA?

NHW SA is a community crime prevention program delivered by the Neighbourhood Watch Volunteers Association of SA Inc. in partnership with SA Police. The vision of NHW SA is to create a safe and connected community.

Local Neighbourhood Watch Areas (like this one) work with local SA Police to help prevent crime. Together we can take action on local issues and help raise awareness of safety and security.

Police Incidents 1 November - 31 January 2024

Date	Location	Details
1. 5/12/23	Windermere Av, CLAPHAM	Items stolen from inside vehicle. Value $240.
2. 24/12/23	Eliza Pl, PANORAMA	1994 Holden Utility stolen. Value $10,000.

REPORTING CRIME

Emergencies

Call Triple Zero (000) in an emergency.

Where life or injury is threatened, or danger to people and property.

Non-Emergencies

Call 131444 for non-urgent police assistance.

For reporting after a crime, reporting a missing person or making police-related enquiries.

Cybercrime

To report cybercrime, or get further information about frauds & scams, visit:

SAPOL: www.police.sa.gov.au/scams

AUSTRALIAN CYBER SECURITY CENTRE

Website: www.cyber.gov.au

IDCARE Phone: 1300 432 273

Web: www.idcare.org

SCAMwatch: www.scamwatch.gov.au

CRIME STOPPERS

Report information about criminals and suspicious activities to Crime Stoppers on 1800 333 000 or at www.crimestopperssa.com.au