



PORTFOLIO REPORTS - STATE COUNCIL

COMMUNICATIONS REPORT

Sally Brindal – Portfolio Holder, March 2024

Telecommunication technology is developing at an exponential rate. While this has resulted in a number of enhancements and improvements for rural and remote communications, the portfolio remains a focus for State Council to guarantee communications services are maintained and continue to be enhanced to ensure our rural and remote students and their families are always provided with adequate communications services commensurate to their needs.

TELSTRA

3G CLOSURE

On 30th June 2024, Telstra are switching off their 3G network; their 4G and 5G networks will be available instead and offer an improved experience. The impact the phasing out of the 3G network will have on rural and remote locations remains a concern for members. Although the 4G and 5G networks have far greater download speeds members question the range of these services and whether it will leave many areas without a phone service.

The following information was provided by Telstra:

- The major determining factor in how far coverage can extend is the spectrum frequency that is used. Lower frequencies reach further and penetrate better into buildings than mid/high frequencies. 4G uses a lower frequency (700MHz) than does 3G (850MHz) which means it can certainly match 3G coverage on a site-by-site basis. There are then maximum limits set by the technology but over the years 4G has been in service, Telstra has raised this maximum in stages with the latest 200km max limit established in 2020 which is sufficient to fully match 3G coverage reach.
- The perception that 4G does not reach as far as 3G is due to several factors that are either misunderstood or will be resolved prior to 3G closure.
- Signal bars on phones are a common source of confusion. 4G operates at lower signal levels e.g. it is more sensitive than 3G. Comparing signal bars between technologies is therefore a misleading indicator of relative coverage with 4G typically showing fewer bars for often better levels of connectivity. Further, there are no standards between device manufacturers for signal bar representation and this only adds to the confusion.
 - Comparisons of coverage and equivalence between 3G and 4G do rely on using like-for-like devices in a like-for-like manner – for example, if you are using a blue tick 3G device you need to use a 4G blue tick device to get equivalent coverage.
- There remain artificial constraints placed on 4G reach to prevent it from extending beyond the edge of 3G coverage. This has been to avoid situations where older non-VoLTE 4G phones (4G phones that only use 3G for voice) can ‘see’ a signal (4G) but be unable to make a voice call. This constraint has been gradually reduced as VoLTE (voice on 4G) device penetration grows and prior to 3G closure will be removed entirely.
- While the vast majority of mobile sites are now enabled with 4G there remain a few hundred that are still 3G only (from a total of 11,000+ sites). Around the fringes of site coverage, and where coverage overlaps between sites, having a mix of 4G and 3G-only sites can be easily misinterpreted as 4G having lesser coverage when that will not be the case once all sites are upgraded with 4G – and this will occur prior to 3G closure.



- Telstra are also using re-purposed 3G spectrum (850 MHz) to support their 5G rollout so they can expand their 5G coverage in regional Australia earlier and more extensively than would otherwise be possible.
- 4G and 5G networks are more efficient than 3G – they can connect more devices, provide higher speeds and have lower latency. They also use the same towers and spectrum frequencies as 3G.
- Telstra’s entire 3G network will remain open until 30th June 2024.

Telstra are conducting detailed checks to make sure their 4G coverage (as they upgrade sites) is equivalent to 3G coverage.

Once Telstra has closed the 3G network they will repurpose the spectrum so that they can use it to expand their 5G network. While it is not quite as simple as flicking a switch, the closure will commence from 1st July 2024 and is likely to happen relatively quickly. Telstra will confirm its closure schedule closer to the closure date, but there will be no loss of 3G coverage prior to 30th June 2024.

What does closure of the 3G network mean for me?

If you have a device that is only able to connect to 3G, that device will no longer be able to connect after the closure date. You will need to upgrade your device before 30th June 2024. This includes customers using 3G mobile, IoT and network extension devices, some EFTPOS machines and antennas that operate on the 3G network only. These customers will be able to continue using their device or antenna until 30th June 2024, but after this date, if the device has not been updated to be 4G or 5G compatible, it will no longer work.

Telstra is committed to upgrading areas that only have 3G coverage to ensure these areas have the same or better 4G coverage available by 30th June 2024. Telstra is committed to providing you with 4G coverage prior to the closure of the 3G network. Your network experience should improve and in most cases, you should notice a substantial improvement in speeds when you move from 3G only coverage to 4G coverage. The 4G service accesses greater bandwidths and is more efficient than 3G, leading to higher end user speeds.

The speed you experience is determined by a range of factors including how close you are to a tower, how much traffic the site is carrying, if any obstructions are impeding the network (i.e., buildings, hills, vegetation etc.) and what sort of device you are using.

Demand for mobile data is growing by around 30 per cent each year.

3G and the Mobile Black Spot Program

All mobile base stations built under the first four rounds of the Federal Government’s Mobile Black Spot Program (MBSP) have 3G and 4G coverage. The 4G network will continue to operate in these areas, even after Telstra have closed the 3G network. Telstra stopped including 3G in their MBSP proposals from Round 5 onwards given their 2019 announcement to exit this technology.

Next G Wireless Link

Several thousand active Next G Wireless Link Service (NGWL) services use 3G technology and they will be migrated to a 4G solution before June 2024. Telstra expects most of these customers will migrate to a 4G fixed wireless solution using the third generation of their Smart Modem (with an antennae port for connections to an external aerial). Existing NGWL customers who already have an external antenna will most likely be able to use it with their new 4G FW solution.

Vodafone closed their 3G network on 15th December 2023 and Optus have announced they will be closing their 3G network in September 2024. For more details check in with the relevant carrier.

CONNECTED COMMUNITIES GRANT



In partnership with the Foundation for Rural and Regional Renewal (FRRR), Telstra's Connected Communities grant program supports organisations providing access to technology, education and facilities that connect rural and regional communities around Australia.

The Connected Communities grant program makes funding available so new or existing not-for-profit programs that help Australians in rural and regional areas get better connected, either through access to equipment, education and workshops or via social networks.

Telstra will make available \$600,000 over three years (the program commenced in 2023) with grants of up to \$10,000 each for community groups that can help build resilient, sustainable and liveable communities. The aim is to help communities connect in whatever way they want, so this is not just about Wi-Fi or stronger phone signals, it may be having someone available to listen and lend a hand when it is needed most.

The program supports local sustainability events and activities, programs that help agricultural groups adapt to changing climate and community e-waste recycling initiatives. It also helps with cyber safety and online awareness, especially vulnerable groups like seniors, students, First Nations people and culturally and linguistically diverse communities. Telstra understands this education is best delivered through the community.

Telstra awards the grants while the program and funds are administered by FRRR. FRRR is a not-for-profit organisation that connects common purposes and funding from government, business and philanthropy with the genuine local needs of rural people and places.

Applications for the 2023 Telstra Connected Communities grant round closed on 30th March 2023 with strong interest received across Australia. The next Connected Communities grant round will open on 1st March 2024.

HOW TO GET FREE WI-FI WHEN OUT AND ABOUT

Since August 2022 about 3,000 of Telstra's Wi-Fi enabled payphones have free Wi-Fi available to anyone and the rest of their 12,000 payphones will offer the same in the next few years.

To connect, find your closest Telstra Wi-Fi enabled payphone or look for the 'free Telstra Wi-Fi' branded payphones. Select 'free Telstra Wi-Fi' in your Wi-Fi settings. Telstra's Wi-Fi portal will launch automatically, agree to the terms and conditions and you will be online.

KEEPING CUSTOMERS IN THE LOOP DURING OUTAGES

Telstra are rolling out new capabilities to keep customers in the loop when they know their services are disrupted.

Telstra customers will now automatically get a heads-up via SMS and/or email to know they are working to fix it. They will then alert them when everything is back online, or if the fix is taking a while, they will get further messages keeping them updated. Telstra can also provide advice on how they can stay connected in the meantime, such as using Wi-Fi calling. After a successful pilot in regional South Australia, Telstra has extended this capability right across regional Australia.

Telstra have also recently refreshed the capability on their Telstra Outages page which will allow you to find out more information on both fixed and mobile outages, estimated fix times as well as planned outages and upcoming planned maintenance using new location mapping tools.

STARLINK

Telstra is working with Starlink to connect more people in remote Australia.



To help provide additional solutions for regional customers, Telstra is now working with Starlink to provide voice and fixed broadband services in remote and hard to reach places using Low Earth Orbit (LEO) satellite connectivity.

This world-first offering means Telstra will be able to provide home phone service and Starlink broadband services to regional Australians as a bundle offer, as well as local tech support and the option of professional installation.

The Starlink agreement will also offer connectivity options for business customers, with a higher bandwidth business option available in areas without fixed and mobile connectivity from January 2024.

UNIVERSAL SERVICE OBLIGATION

The Federal Government recently announced it would consult with regional Australia on how the Universal Service Obligation (USO) can be modernised. Telstra has long advocated that the current arrangements for the USO should be reformed, and specifically making the Universal Service Guarantee (USG) technology-agnostic. They would like to see a focus on delivering the services to our regional and remote customers using new and modern technologies, rather than a continued reliance on technologies approaching the end of life, such as a copper line.

Telstra is focused on getting the connectivity mix right in the regions. For many people in remote areas this will mean having access to services that utilise satellite coverage – something Telstra is currently working hard alongside Starlink to deliver for customers. It will also mean being able to use affordable new products such as Wi-Fi extenders available through Telstra technology partners like Zetifi.

TELSTRA'S NEW DISASTER RESPONSE PUBLIC AWARENESS CAMPAIGN

Telstra began a new disaster response public awareness campaign in November 2023, which included a range of new initiatives to support Australians.

Along with the temporary infrastructure, generators and disaster recovery experts Telstra regularly deploys, the new campaign highlights the following new initiatives:

- Extra data is automatically granted for postpaid mobile customers in a disaster-affected area.
- The upgrade of 1,000 payphones in disaster-prone areas, with free Wi-Fi, USB charging and backup power.
- Reaffirming their commitment to temporary emergency roaming and their intent to conduct a simulation to test its feasibility.
- Launch of the Telstra Response Team – a new way to identify our teams on the ground or at the end of our dedicated disaster assistance line.
- Trialling portable satellite technology that can help local communities connect when mobile and fixed connections are down in a disaster area.

Giving You More Data Automatically in a Crisis

This year, customers on Telstra monthly mobile plans will automatically receive 100GB of extra data on their service if they are in an affected area. As long as your mobile service is registered to an area where disaster assistance is available, you will receive a text message informing you that you will be set up with the extra data for use in Australia within 30 days. Previously, you would have to phone Telstra to get the extra data activated on your account. Now, they are adding it to your account automatically.

Upgrading 1000 Payphones in Disaster-Prone Areas

A few years ago, [Telstra made their payphones free for anyone who needed them](#). Then they went a step further and switched on free Wi-Fi at some payphones. Now, Telstra is working to upgrade 1000 payphones



in disaster-prone areas around Australia to help keep you connected during a disaster. This includes upgrades for 70 remote Indigenous communities. The upgrades provide technology like USB charging for your devices and free Wi-Fi connectivity (to those that do not already have it) so customers can get online, as well as backup power. Telstra has already started these upgrades and is working toward having all 1000 payphones upgraded by mid-2025.

Telstra Response Team

The Telstra Response Team is a dedicated crew of technicians across Australia who will be deployed during a disaster to repair critical equipment (such as telephone exchanges, mobile towers, cables, etc) and restore connectivity to communities affected by disasters. The team is also made up of specialised disaster assistance agents who can help with payment support, advice on how to manage your services if you have had to leave home or resolve faults caused by the disaster.

Testing Emergency Roaming

In an Australian first, Telstra will test the ability for people to use any available mobile network during natural disasters if their own provider's network has been impacted or does not have coverage.

With the number and severity of natural disasters increasing, industry and government have been discussing the technical and commercial hurdles that will need to be overcome before emergency roaming can be introduced. To help guide that conversation Telstra is conducting a simulation within their own network as a first step to demonstrate it is possible.

Telstra will continue to engage with other network providers and Government on emergency roaming, including how it will operate and be funded, as well as the timing for roll-out.

TELSTRA SWITCHES ON FREE CALLS TO SANTA

This Christmas saw the return of Telstra's Free Calls to Santa hotline from any of their 14,500 payphones around the country for Aussie kids (of all ages).

Kids across Australia simply dialled #HO HO HO (#46 46 46) at any Telstra payphone to speak with Santa until Christmas Eve. Kids across Australia were able to do more than just talk to Santa about their Christmas lists, from asking about the weather in the North Pole, to what the reindeer like to snack on before their big Christmas Eve adventure, making the Free Calls to Santa hotline more interactive this year, allowing kids young and old to have more engaging conversations with the jolly man in red.

TELSTRA BIGPOND

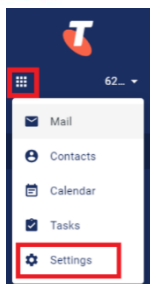
Despite the rumours, Bigpond email is not going anywhere and they do not have plans to stop providing this service.

Telstra has invested around \$20 million this year to upgrade its Bigpond email platform. They are almost done moving more than two million email customers onto this new platform that is more reliable and more secure to make it an even better experience.

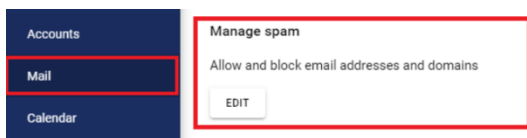
Telstra has spam filters that block some email addresses which are recognised as scams. To avoid important email addresses being blocked by a spam filter please add your email address to the Safe Senders list.

How to add safe senders and block emails

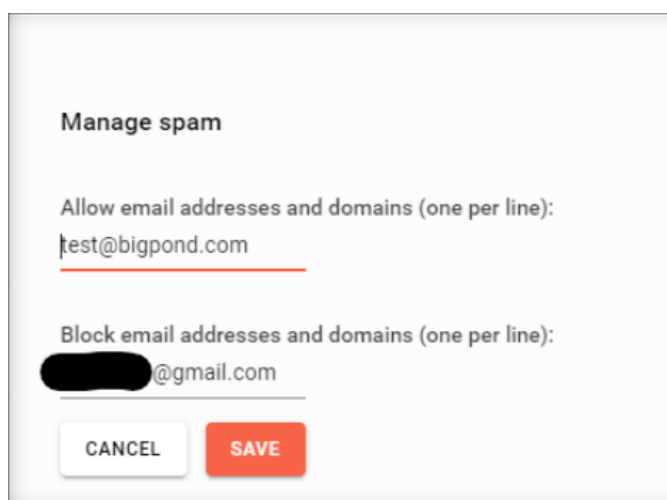
1. Select the squares next to the email address in the top left and click **Settings**



2. On the left side panel select Mail and find Manage spam. If any current safe senders/blocked were added manually, they will display here. To create/add a new one, select **Edit**.



3. The following box will appear. Email addresses can be added to the allowed addresses which would be Safe Senders and if you wish to block email addresses, add them to the Block list. Once the email addresses/domain has been added - click **Save**



WA REGIONAL ADVISORY COUNCIL

ICPA (WA) State Council have an honorary position on the Telstra WA Regional Advisory Council (WA RAC). The WA RAC established in 2017, focuses on:

- Helping to ensure Telstra meets the needs of rural and regional stakeholders and customers.
- Providing input into the activities and plans of Telstra where they involve regional and rural communities.
- Bringing to Telstra's attention important issues facing rural and regional people and communities.
- Deepening understanding of the opportunities, risks and implications of new communications technologies; and
- Identifying and supporting relevant network and connectivity opportunities.

There are up to four meetings each year, including one regional trip. The board consists of members from grass roots organisations: Fresh Produce Alliance, Western Roads Federation, WA Farmers, Sweeter Banana Co-operative, CEO Regional Chambers of Commerce WA, Commissioner, WA Planning Committee and Statutory Planning Committee, an Aboriginal cultural and community leader and various Telstra representatives. There are RAC's in other states with ICPA representation.



On 22nd May 2023, I attended our first face-to-face meeting in over 2 years, in Perth, with Vicky Brady, the new Telstra CEO joining us for dinner. Telstra provided an update on regional communications including how emerging technologies will deliver connectivity in regional and remote Australia, with a particular focus on Low Orbit Earth Satellite (LEO sat). Boyd Brown, Telstra Regional General Manager and Eva Colic, Telstra Regional Engagement Manager, provided a local and community update and the success of the communications for the Solar Eclipse event in Exmouth. A small amount of time was spent on Telstra's regional policies followed by a round table discussion with RAC members discussing their members' issues.

PASSWORD SECURITY

Recent research with YouGov found that almost half of all Australians (46%) use an easy-to-guess password that contains either their favourite sporting team, pet's name or their birthday.

Of those people, 20 per cent have used their pet's name, a further 17 per cent admitted to using their birthdate as – or in – their password and another 9 per cent said they have used their favourite sports team.

Using these passwords makes it especially easy for hackers to access your accounts and personal details without too much guesswork. It is like plastering your password around town for the world to see.

Top Tips for Password Security

1. Use a password manager.

Huge lists published online containing millions of hacked usernames and passwords increase the chance that criminals will compromise accounts with reused passwords. These attacks occur at scale. Criminals can automatically cycle through thousands of compromised logins until an attempt is successful.

This is where a password manager helps. These set and store highly complex, random and unique passwords inside a secured service that is protected with the only password you need to remember. Set one password and forget the rest.

There are many free and easy options available, but you may find it easiest to use the built-in managers you may already have. [Apple's iCloud keychain](#) password manager is built into iPhones, iPads, Mac OS, and the Safari web browser. [Google's](#) password manager is built into Android-based phones including Pixel and Samsung lines, tablets and in the Chrome web browser. Web browsers Firefox and Edge also contain a built-in password manager, while separate free and paid apps exist that work across all mobile devices and computer operating systems.

2. A good password is a sentence.

For decades we have all been taught to use passwords that are hard to remember and often easy for computers to break. Likewise, we have all become used to requirements to set passwords with an upper and lowercase letter and a special character which ends up with people setting predictable passwords such as P@ssw0rd1 or Summer2020! and hackers know it.

So, make the last password you need to remember for your password manager one that is strong but easy to remember by using a passphrase that is unique to you. Write it as a normal sentence, complete with spaces, and throw a number and a few capital letters somewhere to make a highly original combination. Do not use cliches like *I hate Mondays* or *famous phrases* as these could be guessed.

Here are a few good examples, but please do not copy these as your own!

- Time for tea at 1:23 (rhyming may help you remember)
- Somewhere, under TR (an altered version of 'somewhere over the rainbow')
- horsebatterystaplertelephone (random unrelated words that have personal meaning)



Don't want to use a password manager?

Managers are in large part a convenient way to set, save and secure your passwords, but they may not be for everyone.

Those less comfortable with smartphones and apps may instead prefer to write down their passwords on paper. This is fine, provided a few steps are followed.

- Never let people you do not trust see your written passwords. In practice, this means never taking your passwords outside, including in a wallet, purse or backpack. About 1.2 million Australians keep passwords in their purse or wallet.
- If keeping passwords only inside your house is too inconvenient, then consider a password manager.
- You should also avoid storing passwords in any online service that is not a password manager, like a digital notepad, as doing so comes with security risks.

Telstra has developed a simple way to help protect yourself online: **Be SUSS**.



NBN

SKY MUSTER PLUS TRIAL

Nbn trialled a new Sky Muster Plus satellite plan from March 2023 until May 2023 intended to deliver 100 per cent unmetered data usage and aimed to deliver faster download speeds of up to 100 Mbps. After one month, early indications suggested the satellite network appeared to remain robust despite an increase in data usage of about 33 per cent during the peak hours of 4pm-midnight. The trial was also extended to include up to around 15,000 eligible participants (previously 10,000).

The trial has now ended with service providers offering unlimited data for approximately \$100 per month.

Sky Muster Plus Premium was the first nbn satellite plan to offer residential and small business customers uncapped data use to cover all their internet activities. Their first ever uncapped data use satellite plan, [nbn[®] Sky Muster[®] Plus Premium](#), which was launched in June 2023, was so well received that it now accounts for over half of their Sky Muster Plus customer base and these users are consuming at least 4x as much data (on a monthly average basis) than their connections on metered plans. The plan has proven to be popular given



users no longer need to worry about managing a monthly data allowance, and it now accounts for 53 per cent of nbn's Sky Muster Plus users.

December 2023, NBN Co launched two new nbn[®] Sky Muster[®] Plus Premium plans introducing even more satellite connectivity options for people across rural and remote Australia.

Key features include:

- **More choice of uncapped data usage:** users can now choose from three plans – uncapped data use for all internet activities – offering more flexibility without the worrying of a monthly data allowance.
- **Different wholesale prices:** helps make the new plans even more accessible for people in regional and rural Australia.
- **New features for remote access:** the option to purchase static IP addresses for Sky Muster Plus and Premium customers (through their service provider).

The new nbn Sky Muster[®] Plus Premium plans are now available to order and join the suite of existing Sky Muster and Sky Muster Plus plans available.

Not all retail service providers offer nbn satellite connections. For further details and to connect with a participating provider, please visit the nbn website: www.nbnco.com.au/skymusterpluspremium.

The three available plans – at entry, mid and high tier levels – offer greater flexibility and choice for customers depending on their needs and budgets.

The new entry and mid-tier plans will be offered to retailers at lower wholesale prices than the existing Sky Muster Plus Premium plan, which was introduced in June this year.

The three plans now available are:

- **Sky Muster Plus Premium – high tier option:** Replaces the current nbn Sky Muster Plus Premium plan and offers uncapped data use* with maximum wholesale speeds of 100/5 Mbps at least once every 24-hour period and an anticipated typical busy period wholesale download speed of 48 Mbps.
- **Sky Muster Plus Premium – mid tier option:** A new plan that offers uncapped data use* with maximum wholesale speeds of 50/5 Mbps at least once every 24-hour period and an anticipated typical busy period wholesale download speed of 31 Mbps.
- **Sky Muster Plus Premium – entry tier option:** A new plan that offers uncapped data use* with maximum wholesale speeds of 25/5 Mbps at least once every 24-hour period and an anticipated typical busy period wholesale download speed of 16 Mbps.

*Fair use policy applies

In addition to the new plans, nbn is also introducing other new features for Sky Muster Plus and Premium users such as the option to purchase dedicated static IP (internet protocol) addresses for users who wish to do things like remotely access their network from outside their property.

Enhancements to nbn satellite services are made possible due to upgrades to the nbn Fixed Wireless network.

UPGRADE OF THE NBN FIXED WIRELESS NETWORK

NBN Co has announced that around 24,000 homes and businesses across regional Australia are now able to access nbn fixed wireless for the first time.

The 24,000 premises that can now access nbn fixed wireless services were previously located within the nbn satellite footprint. The locations were chosen based on their proximity to existing nbn fixed wireless towers, with priority given to those in the most heavily used parts of the nbn satellite footprint.



Key to the upgrade program is enabling an additional 120,000 homes and businesses in the satellite footprint to be able to access nbn fixed wireless, as well as introducing enhanced speeds during the busiest times of the day over the overall fixed wireless network and two new higher speed plans by the end of the program. The upgrade is being funded by a \$750 million investment, with \$480 million from the Australian Government and \$270 million from nbn. This is part of a nationwide upgrade program to deliver better broadband for homes and businesses across regional and remote Australia.

SCHOOL STUDENT BROADBAND INITIATIVE (SSBI)

To boost education opportunities and narrow the digital divide, the Australian Government is providing up to 30,000 eligible families with no internet at home a free National Broadband Network (NBN) service. Originally a 12-month commitment, the initiative has been extended so the period in which a family can nominate to receive a free service is up to 31st December 2024.

The duration of free services will continue until 31st December 2025 for all existing and new families.

The Government has invested \$8.8 million to support NBN Co's implementation and delivery of this targeted affordability measure. This includes an additional \$4.3 million from the 2023–24 Mid-Year Economic and Fiscal Outlook (MYEFO) to extend the free services to 31st December 2025.

To be eligible, a family must:

- Have a child living at home who is enrolled in an Australian school.
- Have no active broadband service over the NBN network.
- Live in a premise where they can access a standard NBN service.
- Not have had an active NBN service during the previous 14 days.
- Families can directly contact the National Referral Centre to have their eligibility assessed or be referred by a participating nominating organisation.

To check your eligibility, follow these simple steps:

- Contact the National Referral Centre, operated by Anglicare Victoria, on [1800 954 610](tel:1800954610) (Mon–Fri, 10am–6pm AEDT), www.anglicarevic.org.au/student-internet.
- The National Referral Centre team will help assess your eligibility for the SSBI, by checking several things including your residential address and current financial situation.
- If eligible, you will be issued a voucher which can be redeemed at any of the participating SSBI retail service providers. The National Referral Centre will also be available to assist with contacting your SSBI retail service provider of choice and providing follow-up support.

NBN DIGITAL SEMINAR SERIES

ICPA (Aust) partnered with nbn to host a series of digital skills webinars exclusive to ICPA members. These events were designed to provide an opportunity to increase digital capability, hear about available nbn updates, and come along to chat directly with nbn representatives.

YOU DID NOT NEED TO BE AN NBN CUSTOMER!!

Webinar 17th August: Sky Muster Satellite Upgrades

Webinar 21st September: Online Safety for Families

Webinar 19th October: In-home Optimisation

Webinar 16th November: Online Safety and Scam Awareness

Webinar 7th December: Smart Devices

The webinars were highly informative with plenty of opportunities to ask questions. Each webinar was repeated over two time slots 11am and 1pm AEST.



ICPA 2023 CALENDAR

Join your nbn local team for a digital awareness presentation.

On the third Thursday of every month, the same discussion topic will run twice per day. Join us at either 11am or 1pm (AEST) to hear more from your nbn representatives and come along to ask questions.

11am-11.45am & 1pm-1.45pm (All times AEST)

| | |
|--|--|
| ICPA National Conference Increase digital awareness series will be launched. | 17th August Sky Muster Satellite Upgrades: nbn is excited with the launch of the new nbn [®] Sky Muster [®] Plus Premium, come along to find out more and get your questions answered. |
| 21st September Online Safety for families: Improve online safety for all family members as we discuss your digital footprint and CyberBullying and being a positive contributor online. | 19th October In-Home Optimisation: • Are you getting the most out of your nbn [®] connection? What is Wi-Fi and what is data? In this session we look at tips to optimise your in-home internet experience. |
| 16th November Online Safety & Scam Awareness: Want to take advantage of the digital world but unsure about scammers? Come along to learn tips and tricks on identifying and avoiding scams. | Early Bird Session (1st Thursday of the month) "Christmas Special" 7th December Smart devices: Have you noticed all the Wi-Fi enabled products? Let's look at the connected devices that are available now, and what might be using in the future? |

>Keep your eye out for the Microsoft Teams Link

© 2023 nbn co ltd. 'nbn', sky muster are trademarks of nbn co ltd | ABN 86 136 533 741

Nbn is planning to deliver a similar digital series in 2024 with improved time schedules.

REGIONAL TECH HUB

Established in 2020, the Regional Tech Hub (RTH) is a centralised resource providing regional, rural, and remote residents with the critical support needed to navigate the complex world of connectivity and technology options.

The Regional Tech Hub provides **independent** and **free** information about digital technologies, services available, equipment solutions, setup and installation.

Two-thirds of Australia's landmass currently has no mobile coverage, despite a third of Australia's population living outside metro cities. Evolving internet and mobile solutions are helping our regions overcome the digital divide; however, they can be confusing.

The RTH aims to address the gap in digital inclusion between regional and metropolitan communities by simplifying the noise, confusion and frustration around phone and internet connectivity. If you answer yes to any of the following questions, then the Regional Tech Hub can help you:

- Do you need to *get connected*?
- Are you wanting to *stay connected*?
- Would you like to *improve your connection*?
- Would you like to be able to *use your connection better*?

People living in rural, regional and remote Australia are encouraged to reach out to the Regional Tech Hub for independent support to address these four questions.

The Regional Tech Hub offers support via its [website](#), a phone support line 1300 081 029 and social media pages [Facebook](#) and X (formerly [Twitter](#)).



Since December 2020, the Regional Tech Hub (RTH) has received close to 200,000 requests for help, including more than 70,000 website enquiries and has helped close to 10,000 people with their mobile and internet connectivity options.

Of the queries received, maximising coverage through the nbn Skymuster Satellite service was the most common advice sought, followed by requests for information on mobile broadband, mobile phone, nbn fixed wireless and nbn fixed line. Many queries are from people living with an unreliable service that is too expensive or does not meet data needs. In most cases there are options available, which the RTH can raise awareness of and ultimately help more people to find the best solution suited to their needs.

SCAMS

Telstra has a new short national number (7226) for customers to report suspected SMS and MMS scams.

Customers who forward SMS and MMS scams to 7226 (SCAM) will help Telstra better protect millions of Australians from receiving harmful SMS/MMS messages that may attempt to trick them into providing their personal information, credit cards, or downloading malicious apps.

Telstra has a [link](https://www.telstra.com.au/exchange/cyber-security-and-safety/cyber-safety/reporting-sms-and-mms-scams-to-telstra---what-you-need-to-know) available (<https://www.telstra.com.au/exchange/cyber-security-and-safety/cyber-safety/reporting-sms-and-mms-scams-to-telstra---what-you-need-to-know>) with simple tips and tricks on how to forward text messages, including video tutorials as well as tips on what to look for in a scam SMS and MMS.

Top 5 scam calls:

- Amazon impersonation: Scam calls about an issue with your Amazon account. They claim funds will be taken from your account if you do not act immediately by providing personal information.
- Banking/finance impersonation: Scam calls, emails and SMS claiming suspicious activity, unauthorised debits or that your account has been suspended. They request personal details to verify your identity.
- NBN impersonation: Scam callers posing as someone from technical support. They claim there is a fault with your internet to get access to your computer and personal information.
- Telstra impersonation: Similar to the NBN scam. Callers pose as Telstra technical support and claim you have issues with your service or internet to access your computer and personal information.
- eBay impersonation: Scammers use a recorded message to claim you have made a purchase that requires a charge to your account. This is to get you to provide personal information.

All five of the top reported scams impersonate trusted and well-known businesses, with scammers often displaying a fake number or sender information on your phone to make the contact look legitimate.

Many businesses clearly state they will not contact you out of the blue or send messages with links seeking financial information or personal details, so always treat these calls with caution.

How To Avoid Scams

- Do not provide your personal information to an unsolicited caller or sender of a message.
- Do not open links in any unsolicited messages you receive.
- If the brand has an app you can use instead of receiving messages consider whether this will work for you. Messages you receive via the app are much more likely to be legitimate.
- Even if a message slips into a legitimate message stream on your phone, double-check it is from the brand concerned.
- If in doubt, always contact the business via their publicly available contact details (or the details on your regular bill or transaction record) rather than the details provided by the caller or in a message.



PHISHING

Hackers are going to great lengths, including mimicking real people and creating and updating fake social media profiles, to trick victims into clicking phishing links and handing over usernames and passwords.

The alert from the UK's National Cyber Security Centre (NCSC) - the cybersecurity arm of the intelligence service GCHQ - warns that the phishing attacks are targeting individuals and organisations in a range of sectors.

The end goal of the phishing attacks is to dupe the victim into clicking malicious links that direct to fake but realistic-looking login pages, where the victim will enter their login credentials providing the attackers with access to their account, which hackers abuse directly or use to gain access to other victims.

Many of the malicious links are designed to look like commonly used cloud software and collaboration tools, including OneDrive, Google Drive and other file-sharing platforms. In one case, the attackers even set up a Zoom call with the victim and then sent a malicious URL in the chat bar during the call. They have also created multiple characters in the phishing thread (all controlled by the attackers) to add the appearance of legitimacy.

CHATGPT AND AI

ChatGPT has captured the internet's attention with millions using the technology to write poems, craft short stories, answer questions and even ask advice - and 'meanwhile', cybercriminals are using it to generate malicious threats through its impressive ability to generate human-like text that adapts to different languages and audiences.

Norton, the consumer cyber safety brand of Gen, warns that cybercriminals can now quickly and easily craft email or social media phishing lures that are even more convincing, making it more difficult to tell what is legitimate and what is a threat.

Norton says its latest Pulse Report reveals that throughout 2022, it thwarted over 3.5 billion threats or around 9.6 million threats per day, and blocked:

- 90.9 million phishing attempts
- 260.4 million file threats
- 1.6 million mobile threats
- 274 thousand ransomware attacks
- Norton AntiTrack blocked over 3 billion trackers and fingerprinting scripts.

In addition to writing lures, ChatGPT can also generate code. Just as ChatGPT makes developers' lives easier with its ability to write and translate source code, bad actors too can manipulate the technology and use it to scam at a larger and faster scale.

While the introduction of large language models like ChatGPT is exciting, it is also important to note how cybercriminals can benefit from and use it to conduct various nefarious activities.

"We're already seeing ChatGPT being used effectively by bad actors to create malware and other threats quickly and very easily," said Mark Gorrie, Asia Pacific Managing Director at Gen.

"Unfortunately, it's becoming more difficult than ever for people to spot scams on their own, which is why Cyber Safety solutions that look at all aspects of our digital lives are comprehensively needed, be it our mobile devices to our online identity or the wellbeing of those around us – being cyber vigilant is integral to our digital lives."

In addition to using ChatGPT for more efficient phishing, Norton experts warn bad actors can also use it to create deepfake chatbots - these chatbots can impersonate humans or legitimate sources, like a bank or



government entity, to manipulate victims into turning over their personal information in order to gain access to sensitive information, steal money or commit fraud.

To stay safe from these new threats Norton experts recommend:

- Avoiding chatbots that do not appear on a company's website or app and being cautious of providing any personal information to someone you are chatting with online.
- Thinking before you click on links in response to unsolicited phone calls, emails or messages.
- Updating your security solutions and making sure it has a full set of security layers that go beyond known malware recognition, such as behaviour detection and blocking.