AUSCSEC

CEO Newsletter – Issue # 4

December in Australia: A time for family, friends, and festivities – but mind the traps.

December in Australia is a busy time of the year, the panic sets in when the calendar goes from 30 November to 01 December as we realise there are now a limited number of days before the holiday period is upon us. The lifting of restrictions due to vaccination rates has given each of us a sense that our freedom has returned, and life as we know it will go on as it did before COVID-19 hit our shores.

This AUSCSEC message is a timely reminder that cybercriminals don't care about your freedoms, and your way of life, they only care about how they can generate wealth from you and how they can use every opportunity to continue to exploit the pandemic. All new opportunities for COVID-19 related phishing and text campaigns will continue and you can rest assured there will be new variants, not the COVID 19 kind, but new tactics, techniques, and procedures (TTPs), patterns of activities associated with the methods that cyber criminals use to exploit you, your family, and your community to gain access to data that can be commericalised or in another way profited from. We need to remain vigilant. We need to ensure we continue to demonstrate good online security practices, particularly during the holiday period we will especially need to have our thinking caps on, albeit slightly relaxed, but still very aware that we need to continue to use cyber awareness training or critical and common-sense thinking skills:

- to identify if the phone call, text, email, or social media message is a legitimate one, are you expecting this call or text and is it unusual to receive an email from this source.
- when opening an email that contains a link, don't click, just think. Do you know the sender of the email? Why would you be receiving an email or text message from this sender? For example, Amazon and CommBank will never send you an email, they may send you an SMS and Qantas will send you an SMS with respect to an upcoming trip.
- To be very suspicious of any requests of you for personal details, bank account details and passwords and particularly if the request has an urgent timeframe attached to it. If the request is claiming to be from someone you would expect an email from, call them and ask if they have sent the email or message; and
- If you are in any doubt, do not respond.

If you own or run a business, protecting your business from malware and other attacks will be paramount:

- Automatically update your operating system; and
- Automatically update your software applications.

Regularly back up your business data:

- Choose the right back up solution for your business.
- Test your ability to restore back up regularly.
- Store a physical backup safely offsite; and
- Don't forget – if you are an industry that has obligations to keep data for a specific period, be aware of what business data you are required to keep and for what timeframe.

Consider implementing Multi-factor Authentication going into the new year if you haven't already done so because multiple layers make it much harder for criminals to attack your business.

Staff training in Cybersecurity awareness is an important line of defense, regular awareness training and a workforce that has a strong security culture will help protect your business from cybersecurity threats.

- Increasing your awareness sharing and seeking out information could keep your head above water. Improved community awareness of cyber security threats can help. Just knowing helps but if you know and you don't do anything about it, then more fool you.

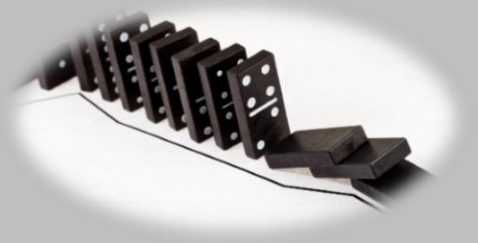
- This year more than ever start building stronger relationships and partnerships with your industry stakeholders and colleagues, start focusing on your supply chain and manage expectations for an event that may happen any time of the year. Understand the boundaries now, so you know who to call for what when it happens during the holidays and every other day.

Cybersecurity threats and trends for 2022

It may come as no surprise to know that you will see more of the same type of cybersecurity threats but using different techniques and methods.

- **Compromised identities** – username and passwords have been the primary source of data breaches over the past year. Alarming really, most people we speak to say they have been the victim of a username password breach. It is concerning that 99% of these breaches could have been prevented. *Remember to change your static passwords regularly and use passphrases, these don't need to be extra-long but need to be something only you would know, this part is within your control.*
- **Ransomware –** Greater focus on disabling data backup capabilities, ensure you have a local and complete copy off site and in a secure environment. Focus on your supply chain management, understand where your supply chain vulnerabilities may be, work with your supply chain third parties to ensure they are secure in their dealings with you.
- **Application Programming Interfaces** (APIs) - Understand what APIs exist in your environment and those of your supply chain third parties. These are the connections that act like a shared boundary across different computer systems so they can exchange

information. Know what boundaries you share with other systems to enable you to exchange information to third parties. Build a community of trust within your supply chain and work closely with your stakeholders to understand where you need to focus your attention. Work with your stakeholders to reduce your supply chain vulnerabilities and your cybersecurity risks.



- Working from home – working from anywhere will still be challenging for any IT security group. Having visibility of user activity will require a mind shift to address the visibility required to improve the overall security posture of an organization. The need to provide strong security controls, high availability to all applications with the lowest privileges for access and data, will drive organizational policy changes in the new year.