MEDIA RELEASE
FOR IMMEDIATE RELEASE

BUSINESS HUNTER

22 December 2022

Cyber criminals target Christmas

With online shopping activity at its annual peak, the region's leading business advocacy group, **Business Hunter** is urging shoppers to be on heightened alert for cyber scams designed to take advantage of the season.

Business Hunter CEO, Bob Hawes said sophisticated scams were anticipating Christmas shopping behaviour and targeting businesses and individuals via email and sms.

"With phones and laptops now the shopping centre of choice for many, and with Christmas shopping in full swing, we're seeing new scams emerge to attempt to trap unwary online shoppers," said Mr Hawes.

"Scams range from sms alerts asking people to pay outstanding delivery charges, to text messages from supposed relatives via new mobile numbers asking for money to purchase Christmas gifts."

Mr Hawes emphasised the need to be vigilant, and not open or click links in suspicious texts or emails, adding that businesses and individuals were both vulnerable to such attacks.

"These schemes are designed to prey on our anxieties and emotions, such as ensuring our gifts arrive safely and in time for the big day or that loved ones can cover their holiday expenses," he said.

Mr Hawes said it was important to think twice before clicking.

"Trust your instincts, if something doesn't seem quite right don't open the sms or email and most importantly don't click on any links. Instead, call the business provider via their listed number or the friend/family on their old number first to follow up," said Mr Hawes.

CEO, Emergence Insurance, Troy Filipcevic said once a malicious link had been clicked it was too late.

"The price you pay could be severe. Your files can be locked down and held to ransom, which is what we saw transpire with Optus and Medibank. For individuals, an attack could result in personal files and precious photographs being stolen or locked down. There is also the risk that they get access to your bank accounts. For a business the ramifications are more broad reaching," said Mr Filipcevic.

Mr Filipcevic said he had seen an unprecedented rise in cyber attacks over the last three months.

“We’ve been in operation for seven years and over that time have seen cyber-attacks steadily increase, but they have skyrocketed over the last three months,” said Mr Filipcevic.

To avoid falling prey to cyber scams, Mr Filipcevic advised the following:

- Remain vigilant regarding emails and text messages. If you don’t expect a package or a communication from the company delete the message
- Regularly ‘patch’ personal devices by undertaking software and OS (operating system) updates – these provide enhanced safety features
- Install Multi Factor Authentication (MFA) – even on social media accounts
- Practise strong password management - don’t use the same password for multiple accounts

Media: Bob Hawes 0418 496 745