NEWSLETTER DECEMBER 2023

venter&hull
CHARTERED ACCOUNTANTS LTD

PROFESSIONAL TRUST.
PERSONAL TOUCH.

Small Business Christmas Checklist

Plan Cash Flow
Make sure your business has enough funds on hand to pay suppliers over Christmas and January, remembering your tax obligations in the first month of the year.

Prepare your cash flow forecasts well in advance and consider holding off on big investments, renovations, and upgrades if things are tight.

Try Christmas Marketing
As we all know, people love to spend money at Christmas, so why not take advantage of the mood with a personalised Christmas promotional campaign? It's not too late to send a marketing email to your customers thanking them for their business - and it can help build brand loyalty.

Review Your Website
Web traffic tends to spike over Christmas, so make sure your website is working well without any glitches before you clock off. E-commerce problems can be hard to fix while everyone is away, so ensure web and mobile sites are up to speed.

Check Your Inventory
Don't guesstimate your inventory or leave things to chance over the summer; make sure your business has enough stock to meet customer demand. Check how much stock you used last Christmas for a guideline.

Sort Out Staffing Schedules
Getting to Christmas and discovering no one is rostered to cover late December and early January is a nightmare scenario. Avoid that worst-case outcome by planning ahead with your staff. Ensure employees take turns to cover the most inconvenient times of the year to keep things fair.

Chase Up Invoices
Chasing up late payments is a pet hate for every business owner. If you have overdue payments in the run up to Christmas, chances are the situation will get even worse in the New Year. Make sure you get paid in full before the summer break.

Get Some Rest
Christmas is an important time to get some well-earned rest, so schedule time to relax! A recent study found that New Zealand workers are more likely to suffer burnout than in any other country. Take the time to reset so you can walk into 2024 with the right mindset.

UPCOMING TAX DATES

20 December 2023
November 2023 PAYE Due

15 January 2024
GST Payments for the period ending 30 November Due

15 January 2024
Provisional Tax Payments Due

20 January 2024
December 2023 PAYE Due

29 January 2024
GST Payments for the period ending 31 December Due

Xmas Closedown

Our office will close at 5pm on Thursday 21st December 2023…

…and will re-open at 8am on Monday 15th January 2024.

From everyone at Venter & Hull, we wish you and your families a safe and happy Christmas season and look forward to seeing you in the New Year.

Best wishes
Renier and Darren

Cybersecurity: New Risks, Fresh Strategies

Cyberattacks are an increasing risk for SMEs — here's how to protect yourself.

Despite the headlines, cybercrime is not all huge data leaks and multi-million-dollar ransom attacks.

According to Forbes, small businesses are roughly three times more likely to be the victim of a cyber-attack. This is probably because smaller businesses tend to invest less in protection measures, making them an easier target for attackers.

More bad news? Cybercrime is on the increase, and attacks are changing. It's no longer just about malware or viruses. Phishing scams, ransomware that disables your systems until a ransom is paid, identity theft and fraud — there are many ways to attack and damage an SME.

As AI use increases, this tech is likely to change cybercrime as well, potentially making it easier for criminals to develop malware and write convincing phishing messages.

Of course, things aren't all doom and gloom. No one tool can protect you against cyberattacks, but some surprisingly effective strategies — both tech and human-focused — can help you build up your protection.

Where do I start?

- Use a VPN
- If you have employees working from home or using their own devices for work, you're relying on random wifi networks to protect your business data.
- Using a virtual private network (VPN) puts a layer of encryption between your data and third-party networks.
- Your employees log in to the VPN before accessing work information and platforms, making it difficult for attackers.

Make protective tech easy

- People won't use protective measures if they're difficult to manage — that's why so many use the same password for everything.
- Make it easy for them by using a password manager to create and store secure passwords, and implementing multi-factor authentication instead of a single password log-in.
- Both these tools add another layer of protection without being arduous or frustrating for the user.

Train your teams

- According to the Harvard Business Review, around 80% of cyber breaches are the result of human error.
- This means raising awareness of cyber threats, investing in ongoing training, and creating a culture of cybersecurity is imperative.
- Your employees should know how to use security measures, identify suspicious activity or red flags for phishing, and know they can approach leadership for help if they're unsure.

Choose providers carefully

- Many small businesses use a loosely-connected network of software, apps and business management tools.
- While this may work for the day-to-day, it can also leave you open to cyberattacks — every piece of tech with access to your business data represents a possible gateway for attackers.
- That's why it's important to screen your providers carefully. Read the terms and conditions, ask about security measures and cloud storage facilities, and don't sign up if you're unsure.
- This is particularly important for AI-driven tech. If SMEs use AI to generate content or analyse data, they need to be aware of the risks.
- Avoid plugging customer data or sensitive business information into these untested tools — and read those Ts and Cs.

Create a security strategy

- If you're running on slim margins, losing funds or access to systems for days or weeks could be devastating.
- To minimise the impact of a cyberattack, you need a protection strategy and an incident plan.
- Your protection strategy should explain your security measures and name your cybersecurity team — including outside experts, internal IT and comms teams and legal or business advisors.
- Your incident plan should include steps to take in the event of a breach, from notifying authorities and shutting down systems to communicating with customers and getting back online.
- If you can minimise downtime and impact of a breach, you have the best chance of recovering and keeping customers.

Weave security into everything you do

- With new attack technology emerging every day, it's almost impossible to create an impenetrable cybersecurity wall around your business.
- But you can build a network of tech solutions and human strategies to reduce as many threats as possible.
- Your business management platform can help.
- Using a single platform instead of a connected network of software means fewer entry points for potential attackers.
- It's also about the tech — use cutting-edge encryption and storage facilities to keep your business data safe.

If you're running a small, potentially vulnerable business, it's a great place to start your security journey. If unsure, get professional advice.

Important: This is not advice. Clients should not act solely on the basis of the material contained in the Client Newsletter. Items herein are general comments only and do not constitute or convey advice per se. Changes in legislation may occur quickly. We therefore recommend that our formal advice be sought before acting in any of the areas. The Client Newsletter is issued as a helpful guide to clients and for their private information.