BusinessPlus+ Newsletter

Issue – April 2021

Business Scams are on the Rise

The ACCC has just reported that Australian businesses reported over $14 million in losses to Scamwatch due to payment redirection scams in 2020, **and average losses so far in 2021 are more than five times higher compared to average losses in the same period last year.** Also note that total scam losses are much higher, as these scams are reported to a range of different organisations.

How Scams Work

Scams targeting businesses come in all sorts of guises and are likely to strike at the busiest times, like the end of the financial year.

- **A false billing scam** is the most common trick scammers use against businesses. Scammers issue fake bills for unwanted or unauthorised listings, advertisements, products or services.
- **The business directory scam** is a well-known example, where you receive a bill for a listing in a supposedly well-known directory. Scammers trick you to sign up by disguising the offer as an outstanding invoice or a free listing, but with a hidden subscription agreement in the fine print.
- **The domain name scam** is another ploy used by scammers, where you are deceived into signing up for an unsolicited internet domain registration very similar to your own. You may also receive a fake renewal notice for your actual domain name and pay without realising.
- **An office supply scam** involves you receiving and being charged for products that you did not order. These scams often involve products or services that you regularly order such as stationery and cleaning supplies. Scammers typically call your business pretending that a service or product has already been ordered.
- **Payment redirection scams** involve a scammer using information they have obtained by hacking your computer systems. They then pose as one of your regular suppliers and tell you that their banking details have changed. They may tell you they have recently changed banks, and may use copied letterhead and branding to convince you they are legitimate. They will provide you with a new bank account number and ask that all future payments are processed accordingly. The scam is often only detected when your regular supplier asks why they have not been paid.

Ransomware can be extremely damaging for any business and is also significantly increasing. The best defence is to back up your data regularly and store your back-ups offsite and offline.

Cyber Checklist

- Don’t agree to offers or deals straight away—always ask for an offer in writing and seek independent advice if the deal involves money, time or a long-term commitment.
- Never provide your business’ banking, financial and accounting details to someone that contacts you unexpectedly and that you don’t know and trust.
- Effective management procedures can go a long way towards preventing scams—have clearly defined processes for verifying and paying accounts and invoices and look very carefully at requests to change banking details.
- Train your staff to recognise scams.
- Back up your business data offsite and offline.
- Beware of emails requesting changes to payment details. Always verify changes to payment details directly with the business or individual - preferably by direct phone communication.

Reporting Business Scams

To report a cyber-crime, visit the business reporting page at **cyber.gov.au.**
More information on scams is available on the Scamwatch website **scamwatch.gov.au**

A useful reference on business scams ("the little book of Scams") can be accessed HERE.

Disclaimer:

Business Plus is distributed monthly by CBSW Tax & Business Advisors to provide information of general interest to our clients. The content of this newsletter does not constitute specific advice. Readers are encouraged to consult their CBSW advisor for advice on any specific business matters.

Providing you professional direction

Our liability may be limited by a scheme approved under Professional Standards Legislation.