TOP TECH SCAMS EXPOSED

DP COMPUTING

DEFENDING SMALL BUSINESSES FROM SCAMS

www.dpcomputing.com.au

Small businesses are often prime targets for scammers due to their limited resources and lack of security. Scammers employ various tactics to deceive and defraud businesses, resulting in financial loss, damage to reputation, and potential closure.

This guide will explore some of the top scams that target small businesses, how to identify them and the steps to protect your business from falling victim.

FAKE INVOICE SCAM

Fake invoice scams involve scammers sending fraudulent invoices to small businesses, posing as legitimate suppliers or service providers. These invoices often appear genuine as they come complete with company logos and contact information. This tricks businesses into paying for services or products they have yet to receive or have not authorised. To protect your business from fake invoice scams:

- Pay close attention to the details, such as the item or services listed, purchase order number, billing address and payment instructions. Compare them with previous invoices from the same supplier.
- Contact the supplier directly using a verified phone number or email to confirm the authenticity of the invoice.
- Be cautious of any sudden changes in payment instructions or requests for payment to a different account.

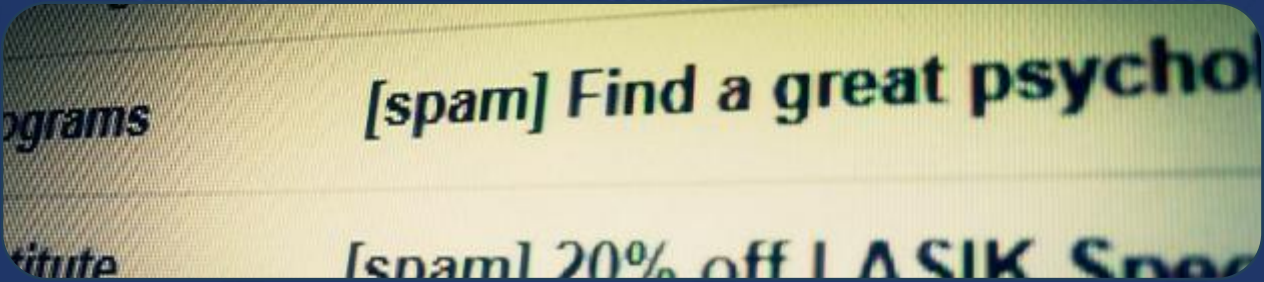
OVERPAYMENT SCAMS

Overpayment scams involve scammers posing as customers who overpay for products or services and then request a refund of the excess amount. However, the initial payment is often made using stolen credit cards or other fraudulent methods. To protect your business from overpayment scams:

- Be wary of customers who insist on overpaying and ask for the excess amount to be refunded.

- Verify the legitimacy of the payment method and ensure that the funds have cleared before issuing any refunds.

- Educate employees about overpayment scams and establish clear refund policies and procedures.



PHISHING SCAMS

Spear phishing is a targeted form of phishing where scammers send personalised emails or messages to individuals within a business, posing as trusted contacts or colleagues. These messages often contain malicious links or attachments that, when clicked, can lead to data breaches, malware infections or unauthorised access to sensitive information. To protect your business from spear phishing:

- Train employees on how to identify and report suspicious emails or messages.
- Be cautious of unexpected or unusual requests, especially those involving sharing sensitive information or clicking links.
- Implement robust spam filters and antivirus software to detect and block phishing attempts.

FAKE SEO EXPERTS

Fake SEO experts approach small businesses and offer their services to improve search engine rankings and website traffic. However, these scammers often use outdated or black-hat SEO techniques that may have short term benefits but in the long term harm your website's reputation and visibility in search results. To protect your business from fake SEO experts:

- Research and verify the credentials and reputation of any SEO service providers before engaging their services.

- Be wary of exaggerated promises or guarantees of instant results. Aa the common saying goes – if it looks to good to be true, it probably isn't true!

- Educate yourself about basic SEO practices to better understand what legitimate SEO services should entail.

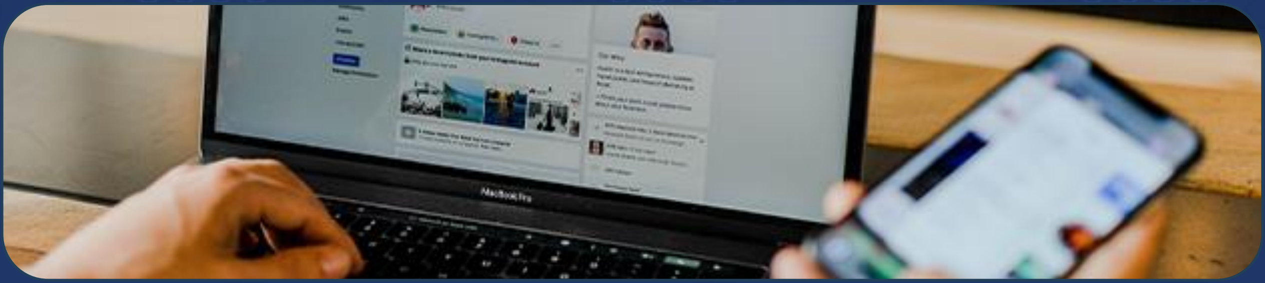
COPYRIGHT INFRINGEMENT SCAMS

Copyright infringement scams involve scammers sending threatening letters or emails to small businesses. These letters claim that you have infringed upon copyrighted material. These scammers often demand payment or threaten legal action if the business does not comply. To protect your business from copyright infringement scams:

- Verify the authenticity of the copyright claim by conducting your own research or consulting with legal professionals.

- Keep records of any licenses, permissions, or original content you have created or obtained.

- Be cautious of any demands for immediate payment or threats of legal consequences.



CHANGED ACCOUNT SCAMS

Changed account scams occur when scammers gain unauthorized access to a business's email or online accounts and change account details, such as bank account information or payment instructions. This can lead to payments being sent to the scammer instead of the intended recipient. To protect your business from changed account scams:

- Pay attention to when such invoices are expected.
- Regularly monitor and review account details and settings for any unauthorized changes.
- Establish strict protocols for verifying and approving any changes to account information.

IMPOSTER SCAMS

Imposter scams involve scammers posing as government agencies, financial institutions or trusted organisations to deceive businesses into providing sensitive information or making fraudulent payments. To protect your business from imposter scams:

- Be cautious of unsolicited communications and verify the request's legitimacy by contacting the organisation directly using verified contact information.

- Educate employees about common imposter scams and establish clear procedures for handling requests for sensitive information or payments.

Small businesses can protect themselves from these scams by staying vigilant, educating employees and implementing security measures. Always verify the authenticity of requests and be cautious of suspicious, different or unexpected communications.

Protecting your business from scams is an ongoing effort that requires awareness, proactive measures, and a healthy dose of skepticism.

For technical security measures, this is where a trusted ally like a Proactive IT Provider like DP Computing comes in. We bring expertise, offering proactive monitoring, robust security protocols and rapid response to emerging threats.

Our vigilance ensures that your business stays ahead in the cybersecurity game, allowing you to focus on growth without the constant shadow of potential scams.

Reach out to us today to talk about how to protect your business.

DP COMPUTING

Reach out to us today to talk about how to protect your business.

Phone:	(08) 8326 4364 (02) 7902 5169
Email:	support@dpcomputing.com.au
Web:	www.dpcomputing.com.au
Facebook:	www.facebook.com/dpcomputing