Australian Competition & Consumer Commission

Factsheet

Business scams

Information for businesses

May 2017

All businesses are vulnerable to scams and they come in various forms—from invoices for advertising or directory listings that were never requested to dubious office supplies that were never ordered. Cyber attackers pose an increasing and serious threat to businesses. They often manipulate employees, access computer networks and masquerade as 'trusted insiders.'

Scammers are causing significant financial loss and reputational risk to businesses through hacking scams and ransomware which are used to obtain personal information or install viruses. Fraudulent payments, email scams and directory fraud are continuing to hurt businesses as scammers have become more sophisticated and go to great lengths to convince you that documents or offers they make are legitimate and genuine.

Common scams to look out for

Overpayment scams

This scam involves scammers contacting you to purchase goods and services then sending you a payment by cheque, money order or credit card for more than the agreed price. The scammer then asks you to refund the overpayment or to pay the scammer's 'freight company'. The scammer is hoping you will transfer the refund or pay for 'freight' before you discover that their cheque has bounced or that their money order or credit cards were phoney.

False billing scams

A variety of false billing scams target businesses—fake directories and advertising, domain name renewal, payment redirection, and office supply scams.

Fake directories and advertising

This scam involves a scammer sending you an invoice by post, fax or email for a listing or advertisement which you did not authorise or request. Scammers may even send a proposal for a subscription, disguised as an invoice or 'renewal notice', for an entry on a fake website or trade directory. It may sound like a 'free' entry, but charges can be hidden in the fine print, resulting in subsequent demands for payment. Scammers may also call to confirm details of an advertisement they claim has already been booked or to offer a 'free trial'—only to find out later that your business has actually been charged for the advertisement.

Domain name renewal scam

In this scam you'll be sent either an unsolicited invoice or email for an internet domain name registration very similar to your own business domain name or a renewal notice for your actual domain name. The notice could be from a business that supplies domain names trying to trick you into signing up to their service or it could be from a scammer trying to take your money.

Payment redirection scams

These 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.

Office supply scam

This scam involves receiving and/or being charged for goods you never ordered or never received, or goods that were not what you thought you agreed to buy. The scammer will call you pretending to be your regular supplier, telling you that the offer is a 'special' or is 'available for a limited time'.

Malware and ransomware

A malware scam involves scammers sending emails or social media messages, or using pop-ups that offer 'free' file downloads, including music, movies and games, or free access to content. If you open the link it may take you to a fake website which asks you to install software to be able to access the content or view the video. If you download the software, your computer will be infected with malware (malicious software). This software allows scammers to access your files or watch what you are doing on your computer. Scammers can steal your personal details and commit fraud, by making unauthorised purchases on your credit card, or carry out other illegal business under your name.

Ransomware is a type of malware that blocks or limits access to your computer or files, and demands a ransom be paid to the scammer for them to be unlocked. Infected computers often display messages to convince you into paying the ransom. Scammers may impersonate the police and claim you have committed an illegal activity and must pay a fine, or simply demand payment for a 'key' to unlock your computer. If you pay the ransom, there is no guarantee your computer will be unlocked.

Phishing scams

Scammers will contact you out of the blue pretending to be from a bank, telephone or internet service provider. They may say that the bank or organisation is verifying customer records due to a technical error. Alternatively, the scammer may alert you to 'unauthorised or suspicious activity on your account' or tell you that a large purchase has been made in a foreign country and ask if you authorised the payment. If you reply that you didn't, the scammer will ask you to confirm your credit card or bank details so the 'bank' can investigate. In some cases the scammer may already have your credit card number and ask you to confirm the 3 or 4 digit security code.

Whaling and spear phishing

The scammer sends a personalised email to a group of employees or specific executive officer, which seems to be from a trustworthy source such as their employer or other staff members, using an email address that looks familiar to you. The email is usually about a fake 'critical' business matter requesting you to take urgent action by following a link to a fake website to provide your confidential company information or financial details, which the scammer will use to carry out fraud. Alternatively, the email may ask you to download an attachment which results in malware being installed.

Investment schemes

This type of scam usually involves telemarketing campaigns peddled as tax-free financial opportunities, to get your business to part with money. These may include sports betting schemes or betting software offers that are nothing more than gambling. Or a scammer may claim to be a stock broker or portfolio manager offering an investment that will provide you with quick and high returns. The scammer might even encourage you to buy shares in a company that they predict is about to increase in value. But the scammer is only trying to boost the price of stock so they can sell shares they have already bought, and make a huge profit, resulting in the share value dropping.

How you can protect your business

There are some golden rules to help you beat scammers:

- Provide your employees with information about scams and how to avoid them.
- If you become aware of a scam, let others know about it.
- Never provide personal information and banking details to anybody you don't know and trust.
- Don't let tactics like bullying, negotiations for a lower price, or charges for unordered or unused goods affect your decision.
- Consider what business information you post on social media and networking sites, as scammers use publicly available information to target businesses.
- Do not agree to offers or deals straightaway—always ask for an offer in writing and consider getting independent advice.
- Keep your filing and accounting systems well-organised—have clear procedures for verifying, paying and managing accounts and invoices.
- Keep your office networks, computers, and mobile devices secure—install computer protection software and a firewall, and change passwords and back up your data regularly.

The Scamwatch website provides further information on the most common scams and how you can protect your business from being scammed: www.scamwatch.gov.au/get-help/protect-your-small-business

What if you are scammed or want to report a scam?

If you spot a scam or have been scammed, report it to the appropriate agency to help them identify scammers and warn others about the scam.

If you've sent money or personal banking information to a scammer, contact your bank or credit union immediately. Or if you suspect you are a victim of identity theft, it is important that you act quickly to reduce your risk of financial loss or other damages.

To find out where to get advice or how to report a scam, visit the Scamwatch 'Where to get help' webpage: www.scamwatch.gov.au/get-help/where-to-get-help.

You can also follow @Scamwatch_gov on Twitter and subscribe via www.scamwatch.gov.au/news/subscribe-to-newsletter to receive Scamwatch radar alerts direct to your inbox.

ACCC 05/17_1208 www.accc.gov.au