Australian Government

ScamWatch
Stop. Better safe than scammed.

Small Business Scams

Scams impacting small business

Scams can happen to anyone. Scammers are sophisticated criminals that target all Australians, and unfortunately small businesses are not immune.

It's important that small business know how scammers work to defraud them and how they can protect themselves, their staff, and their customers.

Common scams to watch out for

Investment

Small Businesses lose more money to investment scams than any other type of scam.

These scams can be very hard to spot – even to experienced investors. Criminals impersonate real investment and finance companies, using technology to create fake financial, legal, and business documents that appear legitimate.

They also create scam investment platforms that look and function like real trading apps. These platforms show fake market data and profit growth to deceive people into believing that their investments are performing well.

Scammers may allow people to make small withdrawals as a means of building trust, but when someone tries to withdraw all their 'profits' they will come up with reasons not to pay.

Read more about investment scams and how to stay safe. ASIC also has information about investment scams on its Moneysmart website.

Payment redirection or Business Email Compromise (BEC)

A payment redirection scam or Business Email Compromise scam is where a scammer impersonates a client, business or employee via email and asks you to make a payment to an account the scammer controls.

This scam often includes an invoice you were expecting (e.g. a large business expense), with modified account and contact details.

The email may be sent from a legitimate business email address that has been compromised (BEC).

A common variation includes CEO impersonation scams, which occur when scammers impersonate the business owner or other senior staff and deceive an employee into transferring large sums of money out of the business' accounts. Scammers will often creating a sense of urgency and secrecy by claiming it relates to a personally or commercially sensitive event.

You can find resources to help prevent and respond to BEC scams at cyber.gov.au.

Buying and selling (products or services) scams

Buying or Selling scams occur when a person is buying or selling a product or providing a service. To make them look genuine scammers may use stolen logos, branding, Australian Business Numbers (ABNs), or a '.com.au' domain name.

These include when scammers:

- pose as buyers, sellers or service providers to steal your money
- create fake websites, digital platform profiles, ads and reviews
- offer products or services at very low prices or that are in rare supply
- request payment for directory listings, advertising, domain name renewals or office supplies that you did not order.

Phishing

Phishing scams are attempts by scammers to deceive you into giving personal information such as a bank account number, password or credit card number, or the details of sensitive business protocols, like payment security procedures. They usually involve a message from a scammer impersonating a known business or person with a hyperlink or request to confirm information.

They may claim to be:

- attempting to verify suspicious activity or transactions
- verifying customer records due to a technical error
- undertaking a customer survey.

Phishing messages are designed to look genuine, and often copy the format used by the organisation the scammer is impersonating, including their branding and logos.

Phishing can also target specific employees and appear to be from a trustworthy source, such as an employer or colleague. Or they can target business owners and more senior staff to steal more sensitive information.

Scammers use the stolen information to hack into your accounts or impersonate you in other kinds of scams and fraud.

Money recovery

If you've previously lost money to a scam, you may be approached by scammers claiming that they can help recover your stolen money. They may pretend to be trustworthy parties like government agencies, lawyers or charities. They might also pretend to be victims themselves, and tell you about a service that helped them get their money back.

Scammers tell you that they can get your money for a fee, a percentage of the stolen funds, or a tax payment. They might tell you they can track down stolen cryptocurrency. They ask you for your personal information. They might ask to access your devices remotely.

Never accept offers from anyone who says they can get your money back, even if they say they are from a legitimate organisation. Work with your financial institution to try and recover your money.

Read more about these, and other scam types at scamwatch.gov.au.

Business impersonation

Business impersonation scams occur when scammers use the name and branding of a legitimate business to steal from them and defraud their customers. Scammers impersonate businesses in different ways including by:

- creating fake replica business websites and fake social media profiles using the branding, logo, and even ABN or industry licence number of the real business
- spoofing the phone number, SMS user ID and email address of a real business making it look as though communications are from the business when they are really from the scammer.

Business impersonation scams cause significant harm. Not only do they result in financial harm, but they may also lead to reputational harm and brand damage through loss of consumer trust and confidence.

Read more about dealing with business impersonations.

The good news is that simple protection strategies work against even the most sophisticated scams. You don't need to understand how these technologies work in detail – there are some simple steps you can take to protect yourself.

Technology used by scammers

Artificial intelligence

Scammers are using artificial intelligence (AI) to create fake videos and documents, clone voices and send personalised messages that are harder than ever to identify as scams.

Spoofing

Spoofing occurs when scammers use technology to make their phone number, email address or SMS user ID look exactly the same as one belonging to a legitimate organisation or person. This means that you shouldn't assume that contact is real, even when it looks like it comes from someone you know and trust.

Remote access

Remote access is most often initiated over the phone. You may also encounter these scams via a web browser pop up instructing you to call a number to resolve an issue.

Victims will be asked to download an app or software that grants the scammer full permission to view and access the device or computer. Once they have control, they steal money and sensitive or personal information.

A common example of this is when scammers impersonate tech support personnel, or a well-known telco or software company, claiming that there is a problem with your device or internet connection.

How to stay safe

Scammers use a combination of impersonation, urgency and emotion to manipulate and deceive. But there are some simple steps you can take to help you stay safe.

Stop. Always take a moment before giving your money or personal information to anyone. Scammers will create a sense of urgency to pressure you into acting quickly. Don't rush to make decisions about money or sharing personal details.

What to do:

- Say no, hang up, or delete suspicious messages.
- Take time to think before responding to unexpected requests.
- Exercise caution when paying an invoice, providing personal or business information, or making a purchase.
- Don't let anyone pressure you into immediate action.
- Trust your instincts if something feels wrong.

Check. Make sure the person or organisation you're dealing with is real. Scammers pretend to be from organisations you know and trust. Always verify who you're really dealing with before taking any action.

What to do:

- Contact the organisation directly using phone numbers or email addresses you find on their official website or app.
- Research investment opportunities or offers through official sources like ASIC.
- Check goods or services were ordered and received and confirm banking details are correct prior to making payment.
- Get a second opinion from family, friends, or professionals.

Protect. Act quickly it something feels wrong. The sooner you act, the better you can protect yourself and others from scammers.

What to do:

- Ensure your staff are aware of scams and put processes in place to protect against scams. Consider using eInvoicing – a standardised, easy and secure way to send and receive invoices.
- Contact your bank immediately if you think you've lost money or shared financial details.
- Report to Scamwatch to help protect others.
- Report to police.
- Monitor your bank statements and credit reports for unusual activity.
- Report the scam to the impersonated organisation and platform where the scam is happening.

Being scammed can feel overwhelming. Support is available at Lifeline or Beyond Blue.

Other cyber threats impacting small business

Malware

Malware is the term used to refer to any type of code or program that is used for a malicious purpose, such as:

- stealing your information and account details
- encrypting your data for ransom (also known as ransomware)
- installing other software without your knowledge.

A malware attack can have serious and ongoing impacts. Malware can also act as an entry point for cybercriminals, opening the door to further malicious activity.

Malware is distributed by:

- spam email or messages (either as a link or an attachment)
- malicious websites that attempt to install malware when you visit
- exploiting weaknesses in software on your devices
- posing as a trusted application that you download and install yourself, such as antivirus or security products.

Read more about cyber threats on the Report Cyber website.

Additional resources

Aside from Scamwatch, there are additional free, Federal Government–funded services designed specifically to support small businesses and boost their cyber resilience.

Small Business Cyber Resilience Service (SBCRS)

IDCARE, the national scam, identity and cyber support service, delivers the Small Business Cyber Resilience Service – a free program for businesses with 19 or fewer full-time equivalent employees (excluding the owner) that are registered in Australia, actively trading, and have a valid ABN.

Cyber Wardens

The Cyber Wardens program, delivered by the Council of Small Business Organisations Australia, empowers small business owners and their employees to become the first line of defence against cyber threats.