# HOW TO IDENTIFY A FAKE WEBSITE

In recent years, Australia has seen an increase in the creation of fake websites. A website can be designed and launched with little effort or skill, due to the availability of website creation software.

Some common fake websites have recently focused on selling expensive items, such as:

- Caravans
- Farm and plant machinery
- Used machinery
- Motorhomes and RVs
- Motorbikes
- Marine outboard motors

NT Consumer Affairs has also identified fake websites selling lower priced items such as boots and puppies, as well as offering escrow or transport services. Escrow is a legal arrangement in which a third party temporarily holds money or property until a particular condition has been met, such as the fulfilment of a purchase agreement. Scammers will sometimes direct customers to an escrow service to make their own website look somewhat legitimate and professional, but both websites will be fake.
By following the below tips, you can help protect yourself from scam websites and identify legitimate websites and shop online with confidence.

## Low, low pricing

By far the best indication of a fake website is the ridiculously low prices. After all, it's the low prices that can attract the most interest, in the shortest amount of time. It also has a tendency to encourage buyers to act impulsively so they can snap up the bargain before someone else.

When scammers launch these websites, they understand that the clock is ticking until the website is identified as a fake and taken down. They need buyers to act quickly and not ask too many questions. They also want their customers to act impulsively and not discuss their purchase with others. The more time a customer has, the more likely they are to research their purchase and talk to someone who may question the pricing and advise them that it's a scam.

Although everyone is familiar with the saying, 'if it's too good to be true, it usually is', it's not always something

that comes to mind when you think you've just landed an absolute bargain.

## Google street view

Fake websites will usually have a fictitious business address, generally well away from major population centres in Australia. This reduces the chances that the customer is able to visit their location to inspect the item they are interested in. The COVID-19 global pandemic restrictions allowed them to have an extra level of isolation, but this is no longer the case. Scammers are always aware of current trends in a country that can be used to cover their activities and encourage engagement. Their focus on selling caravans and RVs was a direct result of their knowledge that international travel had been closed and that Australians were focused on doing long driving holidays instead.

Google Street View is great resource for checking out the legitimacy of a business address. All you need to do is open up Google Maps and type in the address that the website has listed. Click on the street view icon and the screen will change from an aerial image to a street view image, looking directly at the address. With many fake websites you won't see a yard filled with the items they claim to sell. Occasionally the scammers have done some homework and the image may show a yard with items that may be similar to the business they are trying to claim to be. However, it will never show a yard with the items AND the business name on a sign out the front. Other times all you will see is a new industrial estate and some people fall into the trap of thinking that Google Maps images are too old and the business has not been photographed since it opened recently. Although this may be the case, it's still a strong indication that not all is right.

A good way to double check is to do an internet search and telephone a genuine business that is located close to the address (e.g. next door). Ask them if the purported business is actually in the location it says it is.

## Keep your computer software up to date

Set your software, programs, applications (apps) for automatic updates.

From time to time, software developers will update the software on your computer and devices, which will make the software more resilient to malware or hacking attempts. When software is initially created, vulnerabilities are hard to determine. Only after time when the software has been attacked, will these vulnerabilities become obvious and can be fixed. As these attacks continue to evolve as time goes on, it is critical that your software is updating automatically.

Most devices (including all their software) usually have a default setting for automatic updates, but it is important to check that automatic updates are activated.

## Buy reputable antivirus software

Antivirus software (also called anti-malware) is a computer program you should purchase for your all your devices that connect with the internet. It is used to prevent, detect, and remove malicious software that can attach to your device and steal passwords, personal information and access your data files. It is important that the antivirus software is set for automatic updates. As new threats are identified, the software will be automatically updated, keeping your devices safe from newly created malicious software.

Reputable antivirus software will send you a warning when a newly created website is suspicious and will ask you repeatedly if you really wish to open it. This software should keep you safe from most fake websites. You can buy and download the software directly from their website, or purchase the software when you first purchase your device. Some reputable antivirus software are Trend Micro, Norton, McAfee, AVG Antivirus, Avast, Malwarebytes and SecureMac.

## Graphic design, spelling, grammar and ridiculous claims

There are some aspects of a website that may point to it being a fake. Bad English is less common than it once was and almost all of the fake websites NT Consumer Affairs has identified recently have almost perfect graphic design layout, spelling and grammar. However, it's still worth looking out for the following:

Graphic design: sometimes the layout of the webpages may look only half finished or not aligned properly. Some fonts may seem too small or too large. Fonts may also be rather unusual for a website claiming to be Australian.

Spelling: with modern spellchecker software, spelling is less of a problem than it once was for scammers creating fake websites. However, these fake websites are sometimes compiled from other websites, so occasionally there will be passages that seem to be out of place. In addition, look out for American spelling or incorrect usage of Australian expressions.

Grammar: Prepositioning of words in sentences within fake websites is often in American style grammar, not what you would expect from an Australian website, especially one selling machinery or vehicles.

Ridiculous claims: the scammers want to allay any fears a customer may have about spending a large amount of money online. They will dream up all kinds of claims and usually use several on the one website. Here are just a few examples:

- Reputable Australian business
- Free delivery
- Awarded Australia's No.1 Tractor & Machinery Dealer in 2021

- Will deliver any machine you want at your location in the shortest possible timeframe (5-10 days)
- For your peace of mind, we provide 12 months warranty for all tractors and will pay for the tractor to be returned if you're unhappy.

## Other considerations

There are many ways to identify a scam website, or at the very least, become suspicious enough not to proceed with a purchase. Here are some other things to consider:

- Check the URL: scammers often use URLs that are similar to legitimate websites, but with small variations. For example, instead of "paypal.com," they may use "paypa1.com." Make sure to carefully check the URL for any discrepancies.
- Be wary of Australian Business Numbers (ABN): an ABN would seem like a good thing to check the validity of. Unfortunately, most scam websites fraudulently use both the ABN and the business name of legitimate ABN holders.
- Look for contact information: scammers often do not provide any contact information, or the information they provide is fake. Legitimate websites will typically have a physical address, phone number, and email address listed.
- Automated messages: when you call the alleged business, there may be a strange automated message asking you to leave your contact details. This is not typical of a modern, professional Australian business.
- Check for security features: look for the lock icon in the address bar and make sure the URL starts with "https://" instead of "http://". This indicates that the website is using SSL (Secure Sockets Layer) encryption to protect your personal and financial information.
- Watch out for unrealistic offers: scammers often use unrealistic offers to lure people into giving them their personal and financial information. If an offer seems too good to be true, it probably is.
- Check for reviews: access independent review sites to check for online reviews of the website. Be wary if there are a lot of negative reviews or if the website has no reviews at all.
- Trust your instincts: if something seems off or suspicious about a website, it's best to err on the side of caution and avoid it altogether. Many people who have been scammed report that they had some sense that things didn't seem right. Follow your instincts!

- Look for a privacy policy: legitimate websites typically have a privacy policy that outlines how they collect and use your personal information. If you can't find a privacy policy, it could be a sign that the website is not legitimate.
- Be cautious of unsolicited emails or pop-ups: scammers often send unsolicited emails or use pop-up ads to direct you to a website. Be cautious of clicking on links in these messages, as they could lead you to a scam website.
- Check the domain registration: use a domain lookup tool to check the registration details of the website. Scammers may use domain names that are recently registered or registered with false information.
- Check the website's reputation: use online tools such as ScamAdviser, Trustpilot or Sitejabber to check the reputation of the website. These tools can provide information on the website's history, user reviews, and potential scams.
- Avoid making payments through unsecured methods: Scammers often ask for payment through unsecured methods, such as wire transfer, prepaid cards or cryptocurrency. Avoid making payments through these methods as it is impossible to recover your funds if you are scammed.

## Learn about scams

One of the best tools to protect yourself from all forms of scams is to understand new and emerging scams. Learn about some of the different types of scams out there and how to protect yourself here.

NT Consumer Affairs reports about emerging scams on our social media platforms. Connect with us and learn more:

Facebook Page

YouTube Channel

It is important to talk to family and friends about scams and share scam information. You may be naturally cautious and not very susceptible to scams, but this may not apply to all of your family and friends. People are more susceptible to scams when they are busy, lonely, stressed, ill or have just lost a loved one.

## Report a scam

If you think you have found a fake website or any other type of scam, you can report it to the Australian Competition and Consumer Commission (ACCC) Scamwatch website.

## Examples of fake websites

Below are several examples of fake websites that have been identified and taken down from the internet. Please note that although there is differences, most of the fake websites do have a similar look and graphic style.