

#ShopSafeNZ Fact sheet



Shopping online is easy and convenient nowadays, but you also need to be careful about who you're buying from, the personal information you're giving out and where you are shopping.

The Domain Name Commission (dnc.org.nz) oversees domain names associated with websites ending in .nz. Netsafe (netsafe.org.nz) takes complaints about harm to individuals on social media platforms and online spaces. We have partnered to provide some tips on how to safely shop online no matter the online place or domain name space.

Today's shoppers take note. Our fact sheet will give you practical tips on how to shop safely online. While internet scams and cybercrime exist, that doesn't mean you need to avoid online shopping - make it a safe online shopping adventure.

With a bit of know-how and awareness of the potential risks you can take the necessary precautions when shopping online.

Online shopping risks

When we buy online, we are at higher risk of some of the following:



Viruses

A malicious link, site, or social media advertisement could easily infect your machine with viruses and malware.



Scams

Fake “sales” or deals too good to be true can trick you into paying for something you’ll never receive, or into buying fake/counterfeit items.



Stolen identifying information

Compromised email, passwords, credit card and bank information may put you at risk of identity theft.



Phishing

You might get emails or texts offering amazing bargains or claiming there’s been a problem with a package delivery. All designed to encourage you to give out your personal information.



Data breach

Your private and confidential information may become publicly available often through poor security practices. It also means that others can use it for personal gain, or to cause harm to a business or individual.

Six safety tips for safer online shopping

So how can you be safer when it comes to buying goods and services? We've put together six simple online shopping preventative tips. Luckily, these are some simple steps you can take to strengthen your online shopping experiences.

1

Does the site's name match the goods?

If the site's address says boats and it sells make-up, the online store is probably fake.

Why

Domain names (the website's address, e.g. the Commission's is dnc.org.nz) can expire or not be renewed. Anyone can register a domain name once it is available again.

Domain names associated with popular websites in the past can be a target for scammers. They may register that domain, build an unrelated website, and scam you.

2

Look and feel

Check images on the website

Are they good quality, consistent in style, or a mismatched set of photos? Do a reverse image search and see where else the image pops up. You can teach yourself how to do this with a search engine search 'how to reverse image search'.

Pay attention to the language

Spelling mistakes and obvious grammar errors can be telltale signs. Inspect all elements on the site and take your time running through some of the other pages. Oversimplified sites can be a dead giveaway of a fake website.

Why

It could be that someone has copied and pasted text and 'borrowed' images from all over the Internet to create a fake online store.

3

What payment options are available?

If the site displays multiple payment options (such as Visa, Mastercard, Afterpay, PayPal), but only one is available during checkout, it is a warning sign!

Why

To look more legitimate and create a false sense of security, fake online stores display multiple payment options but only let you choose one.

4

Research the seller or company

Anyone can set up a shop online, so it's important to research a company or seller before buying from the site. You can check if the business is registered on the companies register and look for reviews on a few sites where other buyers can share their experiences. Check for scam reports and reviews. See if they have a social media footprint and what that says about the brand. Search online the name of the website or business with the terms "scam" or "review" after it.

Why

Chances are, if the site is a scam, others have already been burned and may have posted reviews online. If possible, it is good to compare reviews on multiple sites and ask family and friends if they have used it.

5

Check contact details, delivery and returns arrangements

Before making an online purchase, check

- Is there a store location, phone number, email address?
- Can you talk to a person, if needed?
- Can you see where your parcel is coming from?
- Are there clear instructions on how you can return your purchase?
- Check social media links. A lot will appear to be unique but will redirect to a businesses main page.

Check contact details, delivery and returns arrangements *continued*

Why

You need to be able to contact the seller if you have any delays, questions or want to return the item. You also need to know where exactly your parcel comes from, New Zealand or overseas, so you can estimate a delivery time and easily return the item without paying excessively for international postage. A physical address in New Zealand is also needed by the Disputes Tribunal in case you want to complain about something later <https://disputestribunal.govt.nz>

Fake online stores are often unclear about their location, use non-standard delivery services and their owners don't want to be contacted.

6

Check the WHOIS information

If the site name ends in .nz, you can find out who the site is registered to on the Domain Name Commission website at <https://dnc.org.nz/>. It is called a WHOIS search.

If the domain name ends in .com, you can use the WHOIS look up service at <https://lookup.icann.org/en>

Why

Have a look at the registration information: are there any discrepancies? Sometimes, when registering a domain for a fake online store, a scammer will add an obviously fake name or address. Use the address to look up the location of the domain name holder on search to confirm it is not an address occupied by someone else, or worse, a vacant lot. Traders must be who they say they are online, so check out those domain registration details! Tell tale signs are also recent registration dates which mean sites may have been registered to make a quick buck.

Additional Resources

Netsafe

www.netsafe.org.nz/plain-language-shopping-and-selling-online

www.netsafe.org.nz/online-shopping

www.netsafe.org.nz/understanding-delivery-scams

DNC

www.dnc.org.nz/assets/Archive-Documents/Safer_online_shopping.pdf

www.dnc.org.nz/blog/deals-too-good-to-be-true-are-probably-a-scam

www.dnc.org.nz/shopsafenz

Still have questions?

If you have questions or complaints about .nz websites, online shopping scams or both – feel free to contact us using the details below.

For .nz domain name queries

involving fake web shops, contact the Domain Name Commission

Email: info@dnc.org.nz

Phone: 0800 101 151 or 04 495 2119
during business hours.

Address: PO Box 11 881

For online harm queries and scams

queries about content hosts (e.g. social media accounts), contact Netsafe

Email : help@netsafe.org.nz

Phone: 0508 Netsafe

Website: netsafe.org.nz