



Public Advisory: Domain Name Fraud

(version 2.0, published January 2026)

South Africa now has more than 50.84 million internet users as at January 2024¹. More than 78.9% of households have at least one person who accesses the internet² and a typical user spends more than eight hours online every day³. Sooner or later, all of these users are going to be confronted with some sort of online fraud. This might be a fake banking website, an email pretending to come from a government department with a valuable tender opportunity, or simply a message from a “relative” who has died and left you a fortune, but only if you give them all kinds of sensitive personal information.

Domain names are the identifiers appearing in email addresses (`fake.name@fakedept.gov.za`) and websites (`www.faketenders.co.za`). This advisory describes a number of fraudulent activities involving domain names and provides some guidance on reporting them to the relevant authorities.

I've found a fraudulent South African website, what should I do?

If you have discovered a South African website that appears to be fraudulent, you may be able to lodge a Take-Down Notice to have that site removed from the internet. A South African website is one hosted by a local Internet Service Provider (ISP), and not necessarily one that ends in a South African (.za) domain name. (Local ISPs can also host .com and other domains, and websites ending in .za can be hosted in other countries.)

The [Electronic Communications and Transactions Act](#) (Act 25 of 2002) establishes a process for members of the public to report unlawful sites to the relevant industry body. ISPA represents many South African ISPs, and has been recognised by the Minister for the purposes of this legislation. A Take-Down Notice can be lodged on [ISPA's website](#). If you are not sure if the site is hosted by an ISPA member, you can select “Unknown” as the target, and ISPA will try to assist in identifying the relevant ISPA member.

If the fraudulent website is not hosted in South Africa, or is not hosted by an ISPA member, you can still try to report the problem site to the company hosting it. Depending on the hosting country, there may be local legal requirements for ISPs to accept and respond to take-down notices. You may need to do some further research depending on the hosting country.

¹ <https://www.statista.com/statistics/685134/south-africa-digital-population/>

² <https://datareportal.com/reports/digital-2025-south-africa>

³ <https://p.widencdn.net/kqy7ii/Digital2019-Report-en>

The Take-Down Notice process is limited to removing content hosted by an ISP. It can't be used to deactivate a domain name, or as a mechanism to obtain identifying information of the party responsible for the content targeted.

I think a .ZA domain name is being used for fraud, what should I do?

The ZA Registry Consortium (Pty) (Ltd) (ZARC) is the custodian of the largest South African subdomains (those ending in .co.za, .org.za, .web.za and .net.za). If you are aware of one of those domains being used for malicious or fraudulent purposes, then you may be able to report that to ZARC.

The [ZARC Anti-Abuse and Takedown Policy](#) identifies the following as abusive practices or uses of a domain name: phishing (counterfeit websites), pharming (maliciously redirecting users), fraudulent websites, distribution of malware, malicious use of fast flux techniques to obscure unlawful behaviour, botnet command and control, spam, distribution of child sexual abuse images, and illegal access to other networks.

Before lodging a complaint with ZARC, please read the [ZARC Complaints Management Policy and Process](#). This document explains which matters ZARC will investigate and which ones fall outside of its scope of authority. ZARC does not generally deal with intellectual property infringements, disputes over the ownership of a domain, or problems with the contents of a website hosted using a particular domain. Please refer to the other sections of this advisory for advice on dealing with those issues.

If you have confirmed that your complaint falls within the scope of matters that ZARC will investigate, you can use [this complaints form](#). Once completed, it should be sent to legal@registry.net.za.

Somebody is using a domain name to pretend to be my company, what should I do?

If your company has an online presence (www.joescompany.co.za) and you discover that someone has registered a very similar domain name (www.joecompany.co.za), with the intention of pretending to be you, then you can pursue a domain dispute with the relevant domain name authority.

For a South African domain name (one ending in .za), the .ZA Domain Name Authority (ZADNA) administers an Alternative Dispute Resolution (ADR) process designed to resolve domain disputes. There are currently two service providers accredited to handle .ZA domain disputes: the [South African Institute of Intellectual Property Law \(SAIIPL\)](#) and the [Arbitration Foundation of Southern Africa \(AFSA\)](#).

Once a dispute is lodged with one of these service providers, it is referred to ZADNA for an initial attempt at informal mediation with the parties. This option is only a possibility if both parties to the dispute are willing to engage in the mediation process. If the parties engage in informal mediation, all discussions and negotiations during the mediation process are confidential, and any settlement is documented in writing, in order to be enforceable. If the

parties do not reach an acceptable resolution within five days, the dispute proceeds to formal review by an accredited dispute resolution provider. There is a cost associated with this process, but ZADNA may be approached by those unable to pay these fees for financial support.

The majority of domains that don't fall under .za are overseen by an international organisation known as ICANN. Most generic domains (such as .com) fall under the [Uniform Domain-Name Dispute-Resolution Policy](#). Your company may need to consult a legal practitioner with specialised knowledge of domain names for assistance if you have a dispute involving a non-.ZA domain.

Of course, there is also nothing stopping you from approaching the courts to seek relief for a domain name dispute.

I've been a victim of online fraud, what should I do?

If you have been a victim of online fraud, then in addition to any of the above steps, you may also wish to report the matter to the appropriate authorities.

If a serious crime has been committed, you need to report it to the SAPS at a police station. Cybercrime, such as online fraud, is still a crime, and must be reported in the same way as any crime that may need to be investigated:

1. Draft an affidavit (sworn statement) which identifies you, the person who has committed a crime (if known), and the relevant facts.
2. Include a clear statement that you require the matter to be investigated further.
3. Take this to your closest police station to lay a charge. Ask for the matter to be referred to the cybercrime division.
4. Make sure you obtain a reference (CAS) number and the details of the detective on duty so that you can follow up.
5. It is important to follow up continuously while being patient and polite – realise it may be up to you to ensure action is taken.

If you don't want to report a crime, but would like to report possible online fraud or suspicious activity, you can use the [complaints form](#) mentioned previously in this document that can be emailed to legal@registry.net.za, with a copy to incident@cybersecurityhub.gov.za to report it to the national [Cybersecurity Hub](#).

I need to request information about a domain registrant for legal reasons

Data privacy legislation prevents the personal information about domain registrations from being made publicly available. This means that if you wish to pursue legal steps against someone who has registered a domain that you believe is being used in an abusive manner, you will not necessarily have ready access to the registrant's details.

If you are a law enforcement representative, a lawyer representing someone in a domain-related legal matter, or someone else with a legitimate reason to gain access to the

personal information of a registrant, you can complete a Data Access Form to request that information. The data access form may be requested from legal@registry.net.za.

How can I tell who is hosting a website?

Many of the processes covered above require that you know which service provider is hosting a particular website. Fortunately, there are numerous tools available online to assist with this, including the following (listed alphabetically, not in any order of preference):

- check-host.net
- Hosting Checker
- iplocation.io
- Who Hosts This

It should be noted that although the domain name record and the website are usually hosted by the same service provider, it is possible for one company to host the domain name record, and for that record to point to a second company that hosts the website. Most of the above tools identify the website host, but if you approach one company with a complaint, and that company indicates that a different company is hosting the actual website, you should approach the second company unless your complaint is limited to the domain name.
