PUBLIC ADVISORY
DOMAIN NAME FRAUD

South Africa now has more than 31 million Internet users[1], more than 64% of households have at least one person who accesses the Internet[2] and a typical user spends more than eight hours online every day[3]. 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 after you disclose 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.

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 Central Registry (ZACR) 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 can report that to the ZACR using this complaints form which should be sent to complaints@registry.net.za.

The ZACR's 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.

---

1. https://www.internetworldstats.com/stats1.htm
2. http://www.statssa.gov.za/?page_id=1854&PPN=P0318&SCH=7652
3. https://p.widencdn.net/kqy7ii/Digital2019-Report-en

PUBLIC ADVISORY
DOMAIN NAME FRAUD

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

If your company has an online presence (www.**joes**company.co.za) and you discover that someone has registered a very similar domain name (www.**joe**company.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 administers an Alternative Dispute Resolution Process designed to resolve domain disputes. Once a dispute is lodged, the registrant will be asked to respond. If the registrant responds, then ZADNA will first attempt to resolve the dispute through mediation. If the registrant does not respond, or if mediation is unsuccessful, then the dispute proceeds to formal review by an accredited dispute resolution provider. There is a cost associated with this process, but ZADNA runs a financial assistance program for those unable to pay these fees.

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.

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 duty detective so that you can follow up.
5. It is important 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 incident@cybersecurityhub.gov.za to report it to the national Cybersecurity Hub.