Public Advisory: Scam/Fraud Websites

Online fraud has been increasing rapidly in recent years. An April 2021 study[1] indicated that 37% of South African consumers had been targeted by fraud relating to COVID-19 in the last three months, significantly higher than the 25% in April 2020. Similarly the number of attempted fraudulent transactions against business increased 44% between March 2020 and March 2021.

The most common fraud schemes targeting consumers are unemployment scams, but many other industries are also the subject of scams, including gambling, financial services, retail, telecommunications, logistics, gaming, online communities and travel/leisure.

The Internet Service Providers' Association (ISPA) operates a take-down notice process (as established in the *Electronic Communications and Transactions Act*, *Act 25 of 2002*[2]) on behalf of its members. This process provides for the reporting of unlawful websites to the hosting providers so that they can be removed from the Internet. In the last quarter of 2020 and the first quarter of 2021, ISPA processed fifty-two take-down notices for South African websites that were classified as fraudulent. These are sites which appear to be designed to trick members of the public out of money, or otherwise cause harm.

Basic steps to protect yourself online

If you are worried that a website you are interacting with may be fraudulent, here are some basic steps you should consider:

1. If it isn't a site you've successfully used before, then do some basic checks online to look for other people's experiences with that site. If you find reports from people who've been scammed, steer clear of that site.

2. Don't pay using a payment system that you can't dispute or reverse if necessary. Most credit cards have a period in which you can reverse a transaction without penalty. That's not true of an electronic funds transfer (EFT). If a website insists on an EFT payment and doesn't offer credit card payment options, that's not a good sign.

3. Don't rely on a phone number or other details listed on a possible scam site to verify that site. Try to search for the company's contact details elsewhere online, or use a directory service to verify that the contact details you see on your screen do, in fact, belong to the company you think they do.

4. If the offer seems too good to be true, it probably is. If you find a special offer on a website you've never used before, and the price is significantly lower than the price for the same thing on sites that you do trust, that's a reason to be cautious.

Make sure that you are aware of the types of scams that are prevalent online. Below are some of the examples of sites that have been targeted by recent ISPA take-down notices.

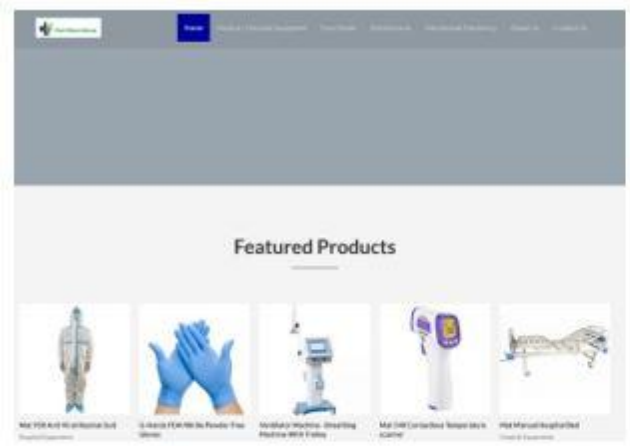
---

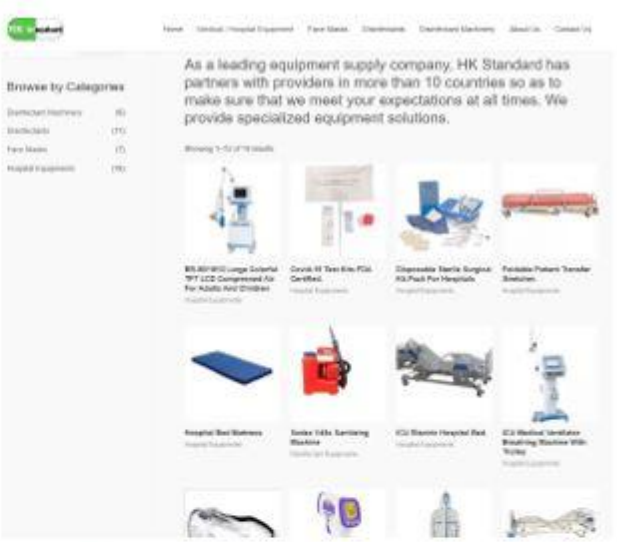
1 https://newsroom.transunion.co.za/one-year-after-covid-19-transunion-research-shows-digital-fraud-attempts-in-south-africa-have-increased-exponentially/

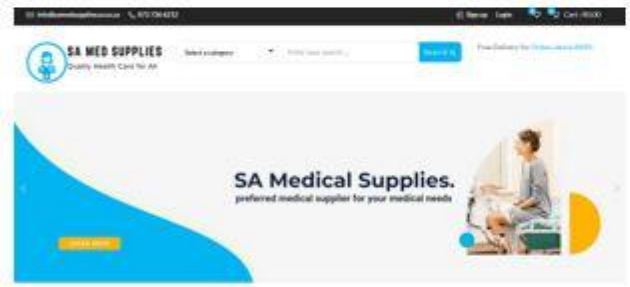
2 https://www.internet.org.za/ect_act.html#Take-down_notification

Medical equipment/PPE

The COVID-19 pandemic has triggered a significant number of fraudulent sites offering medical equipment and personal protective equipment. These sites are often used for tender fraud, listing items with unique part numbers. Fake tender opportunities are sent to companies via email, and the only place they can find the listed parts will be on the fake website.

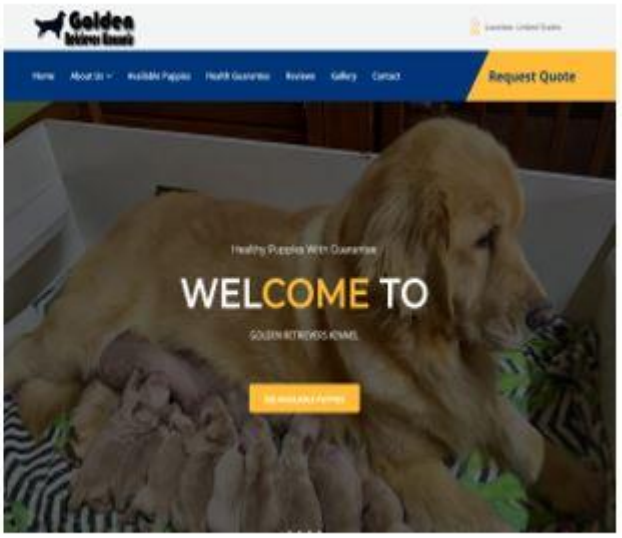






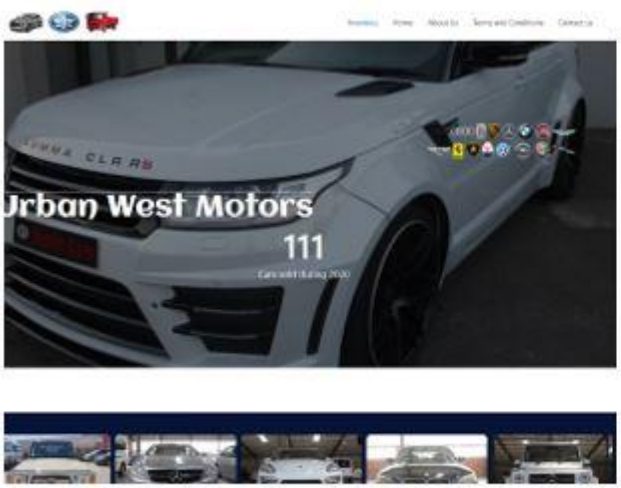
Pets/animals

The SPCA has warned consumers against buying pets online. Many online pet shops are simply scams using stock photographs of "pedigree" puppies and kittens to part you with your money. Anyone sending money to these companies will never receive an animal. However, there are also a smaller number of sites that do provide pets, but where these animals are bred in terrible conditions. Please consider visiting the SPCA or another animal welfare organisation if you want to adopt a pet. This category of scam sites also includes sites pretending to sell poultry and supplies for poultry farming.



Vehicles

Cars and other vehicles are a popular target for scam sites because they involve large sums of money. These sites pretend to have a selection of used vehicles at surprisingly low prices, but never deliver. Often, the fake seller insists on the buyer paying some sort of deposit or down payment to secure the vehicle, but once this is paid, all communication stops. If an online vehicle company does not have a location you can visit to see the car you are interested in, it may well be a scam.

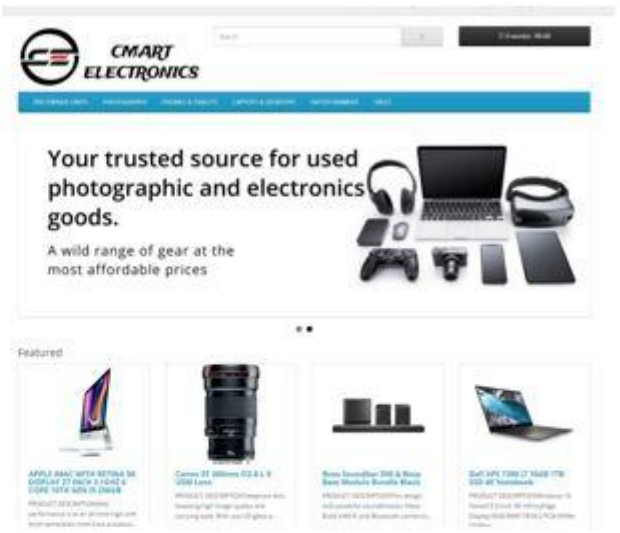


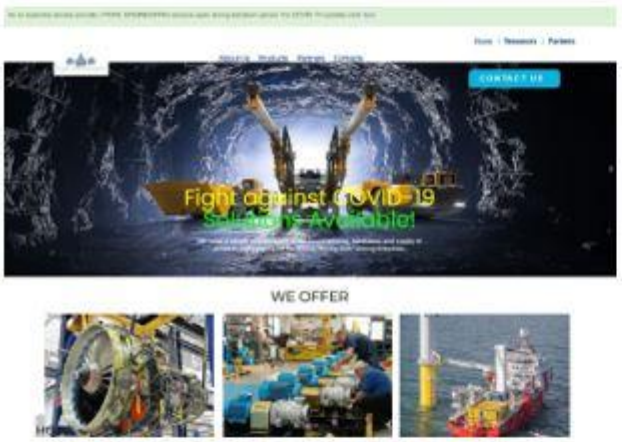
Financial services

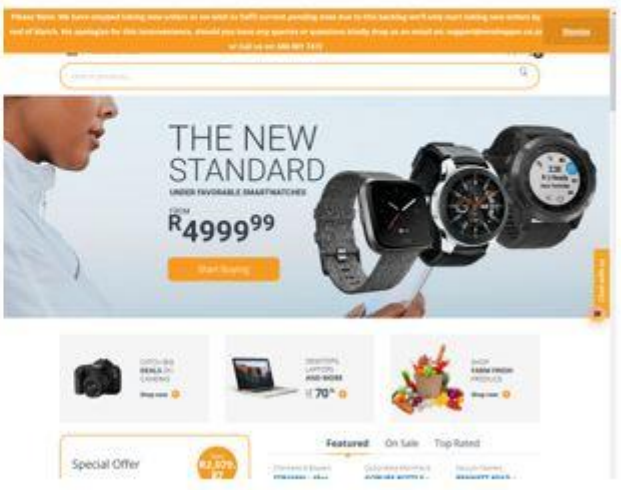
Fraudulent financial websites pretend to be the websites of legitimate service providers, often copying the logos, branding and sometimes the whole contents of the real service provider's website. Customers who provide their personal information to these sites may find that it is used to hijack their bank accounts, or will find that deposits made to open new accounts or pay for financial services vanish without a trace.

Other goods and services

Fraudsters will target almost any products and services with scam websites. Recently removed sites have offered clothing, electronic equipment, generators, industrial equipment and construction services. Wherever possible try to confirm the contact details for a company you are thinking of buying from online somewhere other than their own website. Search the Internet for reports from other people who may have been scammed by that site before you hand over any money.

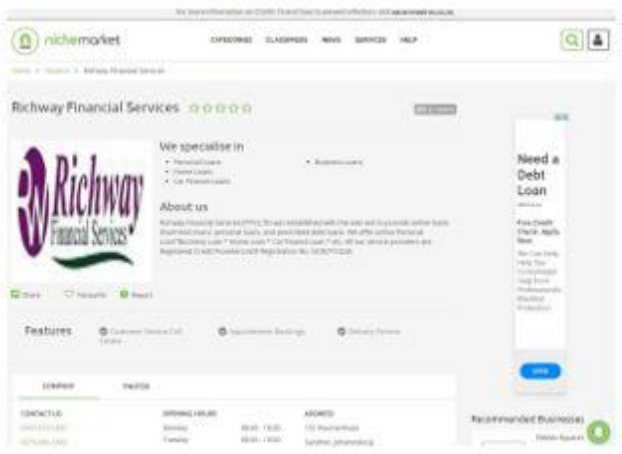


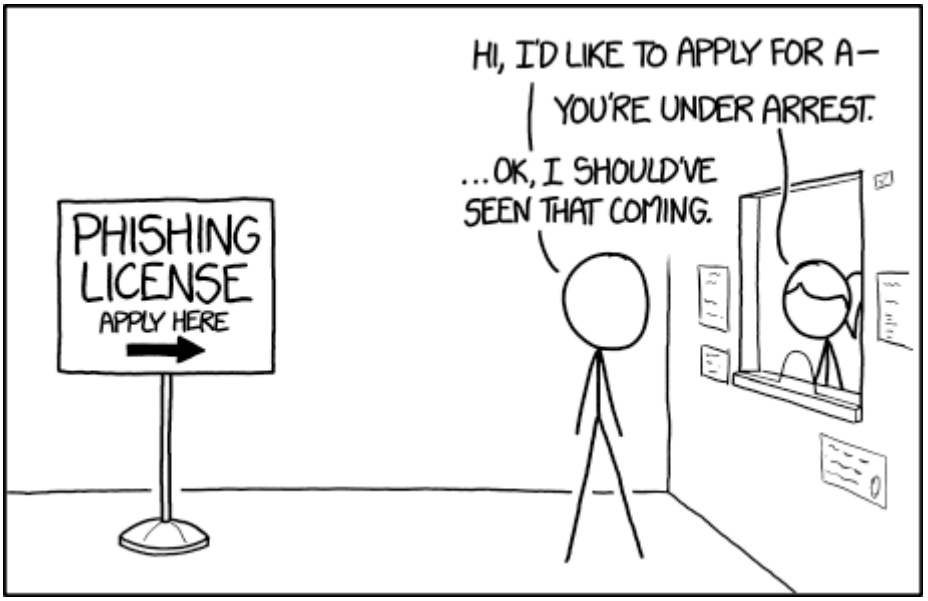




Employment

It is no secret that unemployment is a significant problem in South Africa. Unfortunately, some scammers prey upon those desperately looking for work. These websites offer recruitment services, which inevitably involve the payment of some sort of upfront registration fee, but don't result in any jobs. These scammers sometimes run services over mobile platforms, charging for a series of "interview questions" that the applicant has to submit (and pay for) using premium-rated SMS messages.





Source: https://xkcd.com/1694/