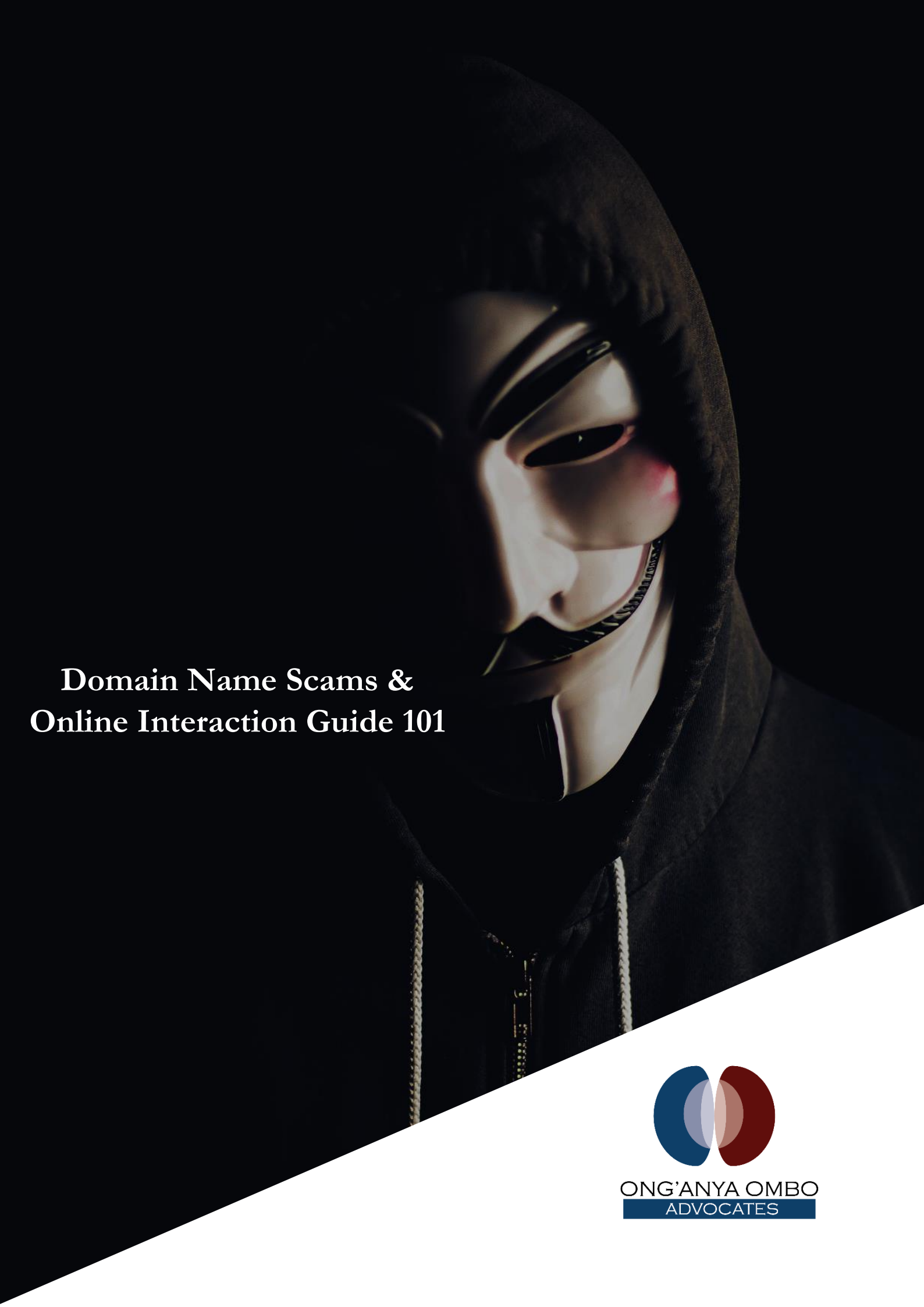


Domain Name Scams & Online Interaction Guide 101

ONG'ANYA OMBO
ADVOCATES

ONG'ANYA OMBO ADVOCATES

Domain Name Scams & Online Interaction Guide 101

A. Domain Name

Domain Name plays an essential role in many businesses – and scammers – today. The purpose of the domain name may include online presence, trademark, custom email address, public relations, control on possible domain name misuse by third parties, domain hoarding/squatting, domain hijacking, phishing, among others. Practices like hoarding or hijacking are prevalent in many developed countries and slowly creeping into developing countries, either effected by people in developed states or ingenious people in developing countries.

Kenya citizens, among other African citizens, need to understand how to interact with domain names – while the remark might seem to look down upon African citizens, it is essential to note that the developed countries are equally facing similar challenges regardless of the developed infrastructure and communication channels. As a result, Ong'anya Ombo Advocates LLP will provide 101 Guide Note on interacting with domain names and related fields.

.com

.org

.us

a) Cautious Approach

The cautious approach simply requires a website visitor or email recipient to be more careful when intending to interact with domain names. A malicious person (MP) understands that issues that trigger a person's mind are related to gifts or money. In that regard, the MP will develop a strategic scheme that informs people that a specific well-known brand is issuing gifts or monetary awards to the public upon taking a particular action. It is important to note that famous brands like Safaricom, Carrefour, EABL, Amazon, Facebook, among others, will use visible models of marketing to access the needed audience and not – for instance – through WhatsApp forward messages, premium rate services, among others.

Once you receive a message indicating that there is an ongoing promotion by these brands or any other company, you need to conduct due diligence, which may include:

i. Check the verified Social Media pages of such companies on whether such a promotion is taking place (some posts addressing such advertisements, if any).

ii. Search online for the organisation's actual domain name; ideally, you search the organisation's name, and it will likely get you the results of the domain name and access it to check whether the promotion is mentioned or being advertised on the website.

   While conducting your online search, be careful as certain organisations may have low brand protection and online visibility; hence, the scammers may even have a better listing based on the Search Engine Optimization (SEO) practices.

iii. You may consider making two to three calls to the company to confirm whether the advertisement or promotion is proper. The option to make two or three calls is to hopefully talk to two or three different customer care service providers for different opinions concerning the advertisement or promotion.

b) Domain Name Scare to Register

Domain Name Scare to Register occurs as a result of the Online Brand Protection. In most instances, big brands or financially stable organisations will register more than 100 domain names; thus, both the country code Top Level Domain (ccTLD) and general Top-Level Domain (gTLD). However, for smaller organisations, those with low budget, less interested in online branding, or lack knowledge on Online Branding are likely to focus on one or a few domain names that can be put to use – and these are the organisations or individuals that are likely to be targeted by individuals

focusing on scaring them to buying domain names that they are not interested in purchasing.

c) Domain Name Authentication

Domain Name Authentication is a process conducted to understand whether the domain name that one is about to access is genuine or the email received from the organisation that one has in mind. Initially, while addressing the "Logical Reasoning," there are initial steps that one can take to confirm the domain name. However, for certain organisations, the domain name might be johndoe.com, but the emails are sent via johndoe.net, email.johndoe.com, or johndoe.app, among other options.

The first step is to use your search engine (search engine includes Google, Bing, Yandex, Yahoo, Baidu, YouTube, Facebook. However, for purposes of this discussion, Google, Bing, Yahoo will be the best options) to check the organisation name, hoping the domain name will appear on the search engine pages and access the link.

One needs to factor organisation's age and domain name age as well. In doing so, it will be odd that a well-established organisation has a new domain or the data in its profile does not relate to the organisation. However, in certain instances, well-established brands will have new domain names; for instance, in Kenya, Barclays Bank Kenya Plc was recently rebranded to Absa Bank Kenya Plc; JamiiBora Bank Limited was recently rebranded to Kingdom Bank; Gulf Energy, Kenol-Kobil were rebranded to RUBiS. It is essential to consider that online scammers take advantage of these opportunities to swindle unsuspecting individuals or organisations during such rebranding processes. For instance, a business using a domain like **waterwatadoe.com** can be malicious represented by an MP as **vvaterwatadoe.com** or **watervvatadoe.com** – in these two examples, the letter "**w**" has been switched to double "**vv**" to make it appear as "**w**" to unsuspecting person. In other instances, the domain **waterwatadoe.com** may be registered with a slight modification with **win-waterwatadoe.com**. whereby the "**win-**" seem to appear as a related or a form of subdomain when it is not related or a subdomain of **waterwatadoe.com**.

Domain Name Authentication can be through:

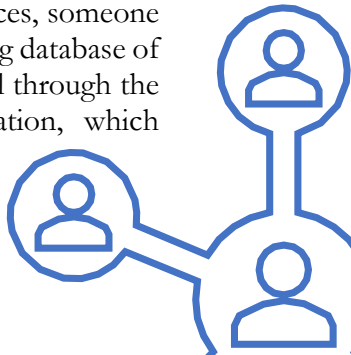
i. WhoIs Search:
   a. ICANN: https://lookup.icann.org – it is suitable for gTLD
   b. Domain Tools: https://whois.domaintools.com – it is ideal for both ccTLD and gTLD

   gTLD refers to .com, .org, .net, .app, among others.
   ccTLD refer to .co.ke, .ca, .ru, co.za, among others.

   In certain instances, it is likely to find that certain organisations have requested the organisation's information be redacted for privacy reasons based on Privacy Laws or internal policies of the domain registrar – and country where the domain registrar is located.
ii. Calling the Organisation.
iii. Checking the Help/ Community Forums of the organisation. Community forums are common in big organisations like Facebook, Twitter, PayPal, Google, among others.

d) Website Verification

Website Verification is quite different from Domain Name Verification; however, verification of one may establish the reason whether to trust or not trust the other – but not all the time. In a few instances, someone might have access to the emailing database of a company and release the email through the official email of the organisation, which



means the domain name will check out; however, at the reply option, the email address is different from the sender's email address, which means that when responding, the owner (victim one) of the account will not know about the communication going on between the third party (victim two) and the scammer.

Once you receive an email, it is essential to check the upper bar of the email to confirm whether the email "from" matches with "reply to." While there are unique instances when there might be a difference, this is not common. Emails with such differences should be treated with caution. Considering that a domain name on "from" differs from "reply to," there is a likelihood that the receiver of that email is about to be scammed or data phished.

Phishing of data and system encryption by ransomware results from such email communications when one clicks a link that either automatically downloads a file that auto-installs in the designated gadget and, if possible, encrypt the servers' of the whole organisation, on the other hand, for phishing purposes, the link will redirect the recipient of the email to a different domain name, probably with slight adjustments from the original domain name, with a website that is better, similar or strikingly similar to the original one requesting the person to key in certain information.

It is important that when such communications are received, the recipient verifies with the relevant organisations, departmental heads, or teammates on whether the email was drafted and sent by the sender/undersigned.

It is advisable to adopt the use reputable Virtual Private Network (VPN) when using internet. The best VPNs are considered to provide the best encryption that blinds the hackers from intercepting in and out flow of data from the gadget.

Ong'anya Ombo Advocates LLP,
4th Floor, Windsor House,
University Way,
P.O. Box 15598 – 00400,
Nairobi, KE.

m: +254 703 672 515
e: hello@onganyaombo.com
w: www.onganyaombo.com