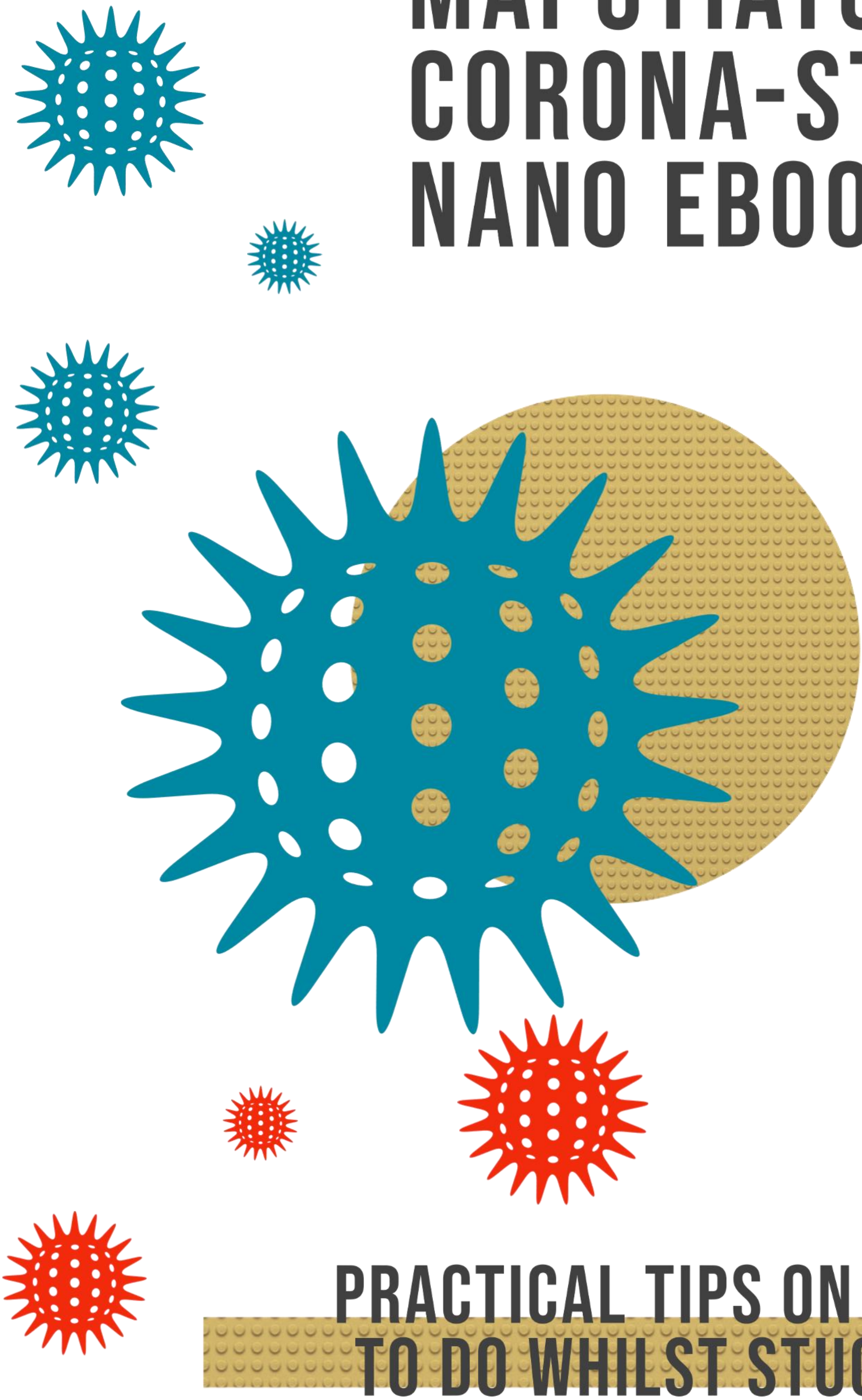
MAPUTIATOTA'S CORONA-STUCK NANO EBOOK 11



PRACTICAL TIPS ON WHAT TO DO WHILST STUCK AT HOME.

Live productively during the
Corona Virus lockdown!

Disclaimer

This publication is designed to provide competent and reliable information regarding the subject matters covered. However, it is distributed with the understanding that the author and publisher are not engaged in rendering medical, educational, legal, financial, social, psychological, career or other professional advice. The author and publisher do not assume and hereby disclaim any liability to any party for any loss of any kind, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Introduction

Welcome back dear reader. Thank you for your consistency! This is the **eleventh** book in a **14 part** nano-ebook series. Just in case you've forgotten, I'm Maputiatota*, and I live in this amazing country, Zimbabwe. Very little content is available about how to live **productively** during the Corona Virus lockdown, and I am on a mission to leave you better than you were when the lockdown began.

Time to DIVE IN!

SECURITY

Every house has rooms with locks and keys. That's security. You lock your doors when you go to bed, and when you leave your house in order to keep your valuables safe.

LOCKS

Data is like a laptop, a gold chain, or any other valuable item. You need to keep it safe. Just like you would keep your valuables safe, you need to "lock" your data in order to protect it from being accessed by unauthorised users. Here are a few methods that can be used to achieve this:

- Passcodes
- Encryption
- Isolating the data (through sandboxes, virtualboxes, etc)

Let's have a look at those methods in more detail.

Passcodes

There are different types of passcodes. The first type uses conventional passwords, then pin numbers, then biometric features. These don't allow access to anyone who doesn't know the passcode. This method has the drawback that the person who manages to "hack" or figure out the passcode will be able to easily gain access to whatever was being hidden from the public.

Passwords

These are simple combinations of letters, numbers and special characters (like !@#$%^&*). A simple password is usually about 8 characters long e.g. chira123

Pin numbers

These are usually a combination of 4 different digits e.g 2222

Biometric features

These use your fingerprint, your iris, your facial features or your voice for allowing you to gain access to the system.

Encryption

This is "locking" your data by using complicated algorithms. What usually happens is you use a passcode which encrypts your data – rendering it useless to whoever doesn't have the passcode. If someone manages to "unlock" your data, through a process called decryption, then your data can be accessed by that clever person.

Isolating the data

This can be done by making sure that nobody gains access to the system. This is done when there is very sensitive data that is present. In this case a person (it's usually an organization though) uses a virtual machine, sandbox, or uses a separate machine which has no connection to any external network – no Wi-Ficard, no Bluetooth card, no Ethernet port.

Ok, you've mentioned security stuff…but why should I care?

Very good question. Houses get raided all the time. Thieves break the locks, and steal the valuables. The same happens to your data.

Really?

Yes. In fact, according to the economist, "The world's most valuable resource is no longer oil, but data"

Your data is valuable. So you better keep it safe.

What can happen?

- Thieves can steal your information and use it to do mischief online. The technological term for this is phishing.
- Crooks can use your passwords to steal money from your bank. All they need is your gmail password. The rest is history.
- And more bad stuff can happen.

How do they steal the data?

Through things called keyloggers. Internet cafés are public places – you don't know the software that's inside the computers. A naughty person can install a keylogger to steal your passwords, and later retrieve them and do naughty things.

Guessing. Yes. Plain old guessing. If your password is newpassword2019 then ANYBODY with free time on their hands can break into your system/account.

They also target accounts online, and if your account has a password like maputiatota1 then it's definitely going to get hacked…sooner or later.

Plain old lying. A person can create an account with an attractive person on the profile. He/She will ask you questions that are used to reset your account. He/She will claim to want to know you more, but once they get the information they need, they disappear into thin air.

What can you do about it?

A lot.

1. Use secure passwords for your gmail account. If this gets hacked, the person will have access to everything. Use a password with a combination of the following:
    - An Uppercase letter
    - A lowercase letter
    - A special character
    - A number

   And make it at least 8 characters long. This doesn't mean that's your maximum. A 10 character password is much more secure than an 8 character password.
   Let's have examples of good passwords:
   Chi$#rat!dz00w
   Mapu#^ti@towt@rr!
   Patakaendakurwizibybetty2020!
2. When using the internet for sensitive things, avoid using an internet café. Buy bundles and create a hotspot. If you can't then when you use the internet, make use of "virtual online keyboards" when entering sensitive information online. Head over to this link to find out more about them.
   PS. The windows virtual keyboard isn't effective at all against keyloggers.
3. And most importantly, don't share your pins. What is the point of having a pin if you're going to share it with everyone. If you have a computer, have a guest account in which anyone has access, then have a private account that has all your information.
4. Don't write your passwords down! Rather, have a memorable phrase so that you won't forget. See it this way – what is the point of locking your house if you leave the keys on the door?
5. Don't install shady applications from shady websites that do questionable things. If you don't know what the application really does AND you installed the application, then perform a virus scan using windows defender. If windows defender finds that app to be questionable, then delete it. Bye bye!

Conclusion

That’s it for today. Tomorrow will be about documents that everyone must have

I hope you enjoyed it. For more material, feel free to head over to my blog https://maputiatotablog.wordpress.com

I’m available on Instagram @ maputiatota, and on Twitter @ maputiatota Don’t be shy to say hi!