VOLUME XI ISSUE 8
AUGUST 2020
OTTAWA ON

# TECHLORE

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

## INSIDE THIS ISSUE:

Cyber Security Practices for your Business Page 1
Gadget of the Month Page 1
The Usefulness of Python in Cyber Security Page 2
What is Ethical Hacking? Page 2
Best Tips for BitCoin Beginners Page 2
Share a YouTube Video at a Precise Point Page 2
How to Get the Most From Your Office's Printer's Cartridge Page 2
Call to Action Page 2

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"
-Jim Stackhouse
NeoLore Networks

# Cyber Security Practices for your Business

If you keep up with the news, you may hear the number of cybersecurity breach cases growing with each passing day. As technology grows more complex and powerful, cybercriminals are looking to profit off of small business poor online security practices that expose vulnerabilities.

A common misconception is that such criminals don't target small businesses because they have bigger fish to fry. Although it's true that large corporations and entities have fallen victim to cyber-attacks in the past, it doesn't mean that small businesses are immune. Cybercriminals are increasingly targeting small businesses. According to a 2019 report by Verizon Data Breach Investigation, 43% of the small businesses were the target of cyberattacks.

### Training Your Employees

Your employees can be the biggest weakness of your business if you fail to train them in implementing best practices for cybersecurity. Imagine if your employees leave their work phone tablet or laptop in a public place. Your business can be in great danger. So, the first thing that you should do is to train your employees. For that, here are some tips for you:

- Share with your employees how cyber incidents can impact on your business.
- You should make the cybersecurity responsibility of every employee.
- Have a regular session regarding cybersecurity.
- Your employees should also know how to respond to a cyber attack.

### Keeping Your Software Up-to-date

Many small businesses neglect to update their applications, which can be a critical threat to your cybersecurity. Cybercriminals and hackers look for weak spots to take control over the data, stealing your important data, or encrypting your files for ransom.

When you update your software, it fixes all security loops to avoid breaches. You should also ensure that the software of the employees working remotely is up-to-date.

### Securing Remote Access

If your employees are working remotely, you need to make sure that their system is secure and safe. You cannot boost your businesses' cybersecurity without updating remote access portals.

### Creating Back-up Files for Critical Data

Even if you follow all the practices for cybersecurity, you might still be a victim of a cyber attack. Hence, you should back-up all the crucial data in a secure place.

Act according to the following guidelines to back-up the data for your small business:

- Keeping your back-up data security up-to-date
- Keep the back-up protected and encrypted
- Storing the back-up on the cloud
- Checking the back-up regularly to make sure that everything is working fine.

### Purchasing Cyber Insurance

Cybercriminals use the latest techniques, software applications, and tools to attack a business. You need to strengthen your cyber defence, but it is still possible that the attacker will find a way to breach your security. To stay safe and protect your small business from any losses, you need to buy cyber insurance.

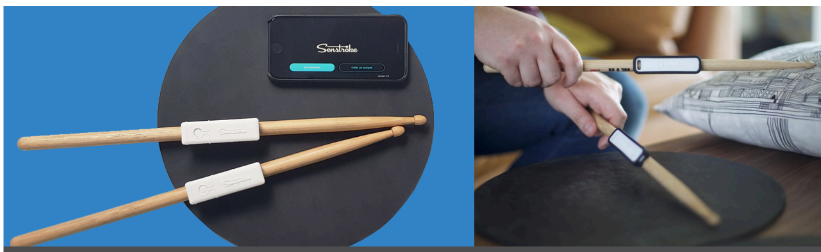
### Investing in Cybersecurity

To grow your business, you have plans, budgets, techniques, and goals. In the same way, you need to invest your time, money, and efforts into robust cybersecurity.

Hackers prefer to target small businesses as they are less protective and have sufficient digital assets. You should buy the latest anti-virus software and other tools for cybersecurity in order to fight back against cyber attacks.

### Conclusion

As cybercrimes are increasing, every small business should focus on its cybersecurity. By practicing the above-mentioned methods, you can keep your defence strong against the hackers.



## Senstroke Virtual Drum Kit

With Senstroke, discover the first connected drumkit that allows you to play, record and progress by playing on any surface. Senstroke has been designed to capture every drumstick's rebounds and feet's vibrations, regardless of your localization and playing surface : whether you play on a table, a cushion, or on your knees, experience genuine drumming sensations! Starting to play with Senstroke is very fast and easy! Get yours at https://www.senstroke.com/

VOLUME XI ISSUE 8
AUGUST 2020
OTTAWA ON

# The Usefulness of Python in Cyber Security

In a world where the online security landscape is constantly changing, security professionals need innovative solutions to respond to threats quickly. But the issue is that almost every popular coding language is complex, hard to understand, and takes time to understand, test, write and execute.

Even educating the teams is hard when they do not have much information about coding and cyber security. However, professionals who are aware of python programming language do not find it difficult to learn, understand, and solve issues related to cyber security. In this article, we will highlight some benefits of using python programming language for cyber security.

### The Usefulness Of Python In Cyber Security

Now, as you know what Python is, we will now discuss the benefit of this programming language in cybersecurity and in what fields you can use it:

### Professionals Can Work Quickly With Python

As there is less to learn in understanding this language, it is becoming the most preferred programming language for people in the cybersecurity field, especially when they have little experience with programming. Even an experienced cybersecurity professional with a technical background can study the basics of this language and start implementing and programming the code quickly.

### Teams Can Be Formed Quickly

When working on a project, cybersecurity teams are easy and quick to form even if no one in the team has a coding background. This is because this language is easy to learn, and you can train the teams quickly. Imagine how much time a team would require if they had to learn a language such as Java. Cybersecurity managers consider benefits like flexibility and ease-of-use and adopt Python for their teams.

### Use Python For Anything As Cybersecurity

Cybersecurity professionals can achieve and accomplish any task and activity with a strong understanding of the concept and using Python code. For instance, Python is broadly used in network scanning, port scanning, accessing servers, sending and decoding the packets, host discovery, and malware analysis. Furthermore, Python is also effective for data analysis, automating tasks, and scripting, which makes this language popular, important, and understandable for cybersecurity.

### Having Extensive Library And Tools

As we have already discussed, Python is easy to use, which makes this language one of the most popular languages among cybersecurity professionals. But the essential benefit is its extensive library. This means that professionals do not have to reinvent the wheel for simple and common tasks. Mostly, they can quickly find penetration testing tools and cybersecurity analysis.

## What is Ethical Hacking?

Hacking is the process of searching for vulnerabilities in a system. After finding these vulnerabilities, cyber criminals gain unauthorized system access and perform malicious activities such as stealing sensitive information or deleting system files. However, if a hacker is involved in finding the weak points of a system to protect it from other harmful hackers, he is an ethical hacker. Identifying and solving potential threats is called ethical hacking.

Ethical hackers follow a few key protocols and concepts:

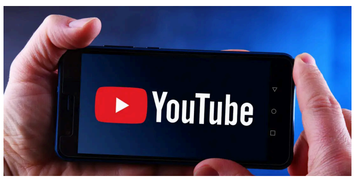
1. Ethical hackers stay legal. They obtain approval before performing and accessing a security assessment.
2. They determine and define the scope of the assessment and work legally within the boundaries of an organization on approval.
3. They report all the vulnerabilities and inform the organization. They provide the best possible advice on how to resolve these vulnerabilities.
4. They respect the sensitivity of the data. All ethical hackers should agree to a non-disclosure agreement before accessing the data. All the terms and conditions in the agreement are according to the organization.

## Best Tips for BitCoin Beginners

1. Keep your wallets separate. You can store your currency in unlimited wallets, so divide your Bitcoins in different wallets if you want to avoid any type of abuse.
2. Avoid using a web wallet for your savings. Sure, web wallets are convenient, but they are also dangerous. To prevent your web wallet from getting hacked into, only keep as much as you will be using in the near future.
3. You should protect your privacy. Keep your financial details, private keys, and your total wallet details to yourself. You can transfer your funds through mixing services.
4. Even if your wallet is not online and on your computer, you are still at risk of cyberattacks. The best thing you can do is to store your private key in an offline medium such as a USB, or QR code, etc.

## Share a YouTube Video at a Precise Point

If you see something in a YouTube video that you want to share at a particular point, you can get a link that takes people directly to that moment, you can get a link that takes people directly to that moment. Click the Share button below the video. Look for a checkbox below the link. It will automatically display the time at which you currently have the video stopped. Copy the link and share it on your preferred social media or email it to a friend.



## How to Get the Most From Your Office's Printer's Cartridge

**Unclog the Nozzle –** Clean the bottom of the cartridge with a damp paper towel and then follow up with a dry paper towel. This way, the output will not be inconsistent.

**Default Settings –** You can save your toner by keeping your print settings on default.

**Print in Grayscale –** If you are printing on color toner, set your printer on grayscale while printing black and white. This will help you prevent the printer from giving you a richer black that uses different colors for a deeper tone of black.

**Change Print Mode –** You can reduce the DPI by choosing the toner-saver mode, fast mode, or draft mode. You can use these modes when the content matters more than quality.

**Optimizing Your Cartridge –** Toner in a cartridge is in powder form. With time, this powder can get uneven and clumpy, which leads to wasted toner, uneven prints, and streaks. To extend the life of the toner, remove the cartridge and shake it to distribute the powder evenly.

## Take the NeoLore Cyber Security Survey

Has your company done a Cyber Security Maturity Assessment within the last year? Do you have an I.T security policy in place? Do you know if you've been hacked or are leaking data?

If your answer was "no" or "I'm not sure" to any of those questions, your company may be at risk for a devastating cyber attack.

Get the NeoLore Networks Cyber Security eBook for Free!

**It Features**

- Information on the various threats to your business
- NIST Security Framework
- CIS Controls
- Basic Controls

And More!

https://neolore.com/cybersecurity