**International Journal of Multidisciplinary Research and Development**
**Online ISSN: 2349-4182, Print ISSN: 2349-5979; Impact Factor: RJIF 5.72**
**Received: 06-11-2020; Accepted: 21-11-2020; Published: 09-12-2020**
**www.allsubjectjournal.com**
**Volume 7; Issue 12; 2020; Page No. 34-40**

# Effects of cybercrime on business organizations in Lusaka district in Zambia

**Phiri Given Gift**
Technical and Standards Officer in Lusaka, Zambia

**Abstract**
This study has reviewed that there are technical and human factors that are impacting either positive and negatively on the effective eradication or reduction of cybercrimes in Lusaka district. Some factors reviewed were:
Rigidity of managers to embrace contemporary approaches in the cyber security eradication in their organisations. This is where administrators were not flexible to allow IT officers implement cyber security methods by using the ICT gadgets in organisations.
The Inability to procure and distribute cyber security gadgets in the organisations by administrators also affected negatively the cyber security in Lusaka district. This impeding factor need to be seriously addressed by the business organisations.
It was also reviewed that 75% of IT officers assigned to look into cyber security did not have ICT qualifications and could not effectively address the challenges faced by education in organisations in Lusaka district.
The research also reviewed that many business organisations in Lusaka district do not have cyber security materials and cyber security skills. This affected implementation of cyber security in in organisations in Lusaka district.

**Keywords:** cyber security solutions, Lusaka district, Zambia

## 1. Introduction
In Zambia many banks have been robed millions of kwacha recently through cyber-crime.
It is against this that this article has been written to warn companies and people in general to be alert as the do business online. The recommendation would be that companies and organization should take keen interest in investing in cyber security and employ highly qualified cyber security officers if their businesses are to be safe online.
The year 2017 saw some of the most devastating high-profile cyber-attacks in the history of business. This happened despite tech giants constantly releasing security patches and updates. As the number of such attacks continues to rise, 2019 requires businesses of all sizes to be even more prepared given that cyber-criminals are not often selective when choosing their targets.

### 1.1 Statement of the problem
Cyber-crime is conducted by hackers to fraudulently robe people in organization and home millions of kwacha through the internet. In Zambia Lusaka district in particular banks, companies and private individuals have been robbed of millions of hard earned money. It is against this background that this research was conducted to find out the extent to which cyber-crime has affected business and individual in Lusaka district. In addition we wish to find the solution to this problem.

### 1.2 Research objectives
The study seeks to achieve its general objective to assess cyber-crime and identify its effects in organizations and individual homes in Lusaka district.

### 1.3 Specific objectives
1. To determine the impact of cyber-crime in Lusaka district
2. To provide the solution to cyber-crime in Lusaka district

### 1.4 Research questions
1. How many organisations and homes have suffered cyber-crime in Lusaka district?
2. What should be done to control the effect of cyber-crime in Lusaka district

### 1.5 Methodology
The study is belt on the foundation of an ontological worldview of conducting research and as such the following will be the research design and methods.

### 1.6 Research Design
This research proposes to use a Quantitative Research Design taking Descriptive Survey Research Method.

### 1.7 Study Population
The target population in this study shall comprise respondents from the Ministry of General Education Provincial Head Quarters (PEO), Zambia Information Communications Technology Authority (ZICTA), the i-school Zambia, Organisation administrators in rural organisations, Class officers in rural organisations and Pupils from these rural organisations

### 1.8 Sampling Procedure
A mixture of both probability and non-probability sampling techniques will be employed in the selection of the sample. From the probability technique, a cluster sampling techniques will be use and from non- probability technique sampling purposive and quota sampling techniques will be used in selecting respondents in the sample.

### 1.8.1 Cluster sampling technique
Organisations in Lusaka district will be sampled by means of using cluster sampling technique.

### 1.8.2 Quota and Purposive Sampling Technique
After organisations are sampled using the cluster sampling technique the combination of purposive and quota sampling techniques will be used in determining the respondents to participate in the survey. Heads of organization and officers from ZICTA, universities and government institutions will be sampled using purposive sampling technique.

### 1.8.3 Sample Size
The sample size will be calculated using one of the many formulas applied survey research designs expressed as in the table below (fox *et al.*, 2007).

**Table 1**

| Require sample size | Formula for an infinity population | | Actual calculations | | | | Expected sample size |
|---|---|---|---|---|---|---|---|
| N = | $\frac{P(100-P)}{(SE)^2}$ | = | $\frac{50(100-50)}{(2.55)^2}$ | = | $\frac{2500}{6.5}$ | = | 385 |

Where in the equation; N is the required sample size, P is an estimated % of respondents who would give desired responses (estimated at 50%), SE is Standard Error of the mean calculated by dividing the confidence interval, expressed as ($\pm$0.05), by the Z value which is 2.55 and Z is the standard score obtained by subtracting mean of the sample from observed value and divided by standard deviation of the sample. This is the statistical value corresponding to level of confidence required which is expressed as (1.96 at 95% confidence level).

### 1.8.4 Data Collection Process
Data is planned to be collected by the researcher through the use of research instruments that will incorporate questionnaire, structured interviews and observation checklists. Research instruments will be administered to participants and respondents with the help of heads of organisations and departmental institutions targeted in this research. In order to uphold the quality of data obtained, it will be ensured that respondents who may not be failure with what they will be required to provide are assisted to provide that which will be to their best of the knowledge and experience without violating the ethical standards in research.

### 1.9 Data Analysis Plan
Plans to analyse collected data fall on procedure of analysing data collected by using descriptive survey research design that shall include the following SPSS descriptive statistics, correlation and regression statistical tools.

### 1.10 Ethical Consideration
The research is aimed at following all laid down procedure in ensuring adherence to the ethical standards in protecting the respondents and participants. Data collection will only take place after permission is granted from the ethical research committee of either the university or an established notional ethical body. Respondents and participants will not be coerced in taking part but consent will sort for and will only do so by own volition and that will not by any means be used against them but purely for the intended purpose.

## 2. Literature Review
A survey by Osterman Research found that ransomware attacks were the most common in 2017, leading to massive losses to businesses from the inflicted downtime. Many businesses had to shut down their systems for extended periods of time – up to 100 hours or longer.

The human element within organizations remains the main point of weakness as far as cyber security is concerned. Negligent employees or contractors result in up to 54 percent of all data breaches. This is up from 48 percent the year before, according to the Ponemon Institute's 2017 report on the State of Cybersecurity in Small and Medium-sized Businesses.

Cybercriminals frequently target the workforce with malicious emails and websites which an employee may easily click on, setting themselves up for malware attacks.

One recommended way to mitigate these kinds of threats is to train employees to practice some level of cybersecurity housekeeping. This can include simple acts such as logging out of their systems, not logging into company databases from unsecured Wi-Fi, as well as keeping their passwords secret.

Reminding employees of the importance of such good cybersecurity practices can go a long way in staving off ransomware and other cyber threats.

Cybercrime continues to become more lucrative, making it more appealing to prospective and current perpetrators. And with the growing sophistication of the tech world, you can expect the tactics that cybercriminals use to evolve.

Expert assessments hold that organizations can strengthen their cybersecurity through some very basic measures. These foundational steps can readily be implemented.

In recent times we've seen a dramatic increase in the use of personal devices in offices, including laptops, tablets and smartphones. If they aren't protected by your company's security network, they can provide an opportunity for hackers to gain access to your company data.

Email phishing attacks are engineered to trick their unsuspecting targets into providing sensitive data and information. The majority of phishing attacks will be sent via spam which is why it's so important that you implement effective anti-spam software such as Mail Cleaner for your business.

Malware is software that has been designed to gain access to or cause damage to a computer without the knowledge of the operator. It's normally sent via email as a link or an attachment. With a $2.4-million-dollar average cost for companies, this is the most costly form of cyber-attack.

### 2.1 Cyber crimes
The following are some startling cybercrime facts that should inform your approach to cyber security in 2020 and beyond. The University of Maryland's Clark School recently found that that 1 in every 3 Americans has already been on the receiving end of a cyber-attack.

Identity Theft is the criminal act of illegally and deceptively assuming the identity of another individual without the

expressed consent with the intent of committing a crime; fraudulent and illicit attainment of personal information through the usage of unsecured websites can be prosecuted through Internet Law.

According to www.zicta.zm/2018, "Hacking is the unlawful entry into the computer terminal, database, or digital record system belonging to another individual; hacking is conducted with the intent to commit a crime". Within the scope of Internet Law, a computer virus is a program created to infiltrate a computer terminal belonging to another individual with the intent to cause damage, harm, and destruction of virtual property Spyware are computer programs facilitating the unlawful collection of data, allowing individuals the illicit access to the personal and private information belonging to another individual Spam is defined as a digitally-based criminal instrument, which involves the unsolicited transmission of electronic communication with indent of committing fraud

**An. SQL Injections**

An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form entry field – most commonly usernames and passwords – to give the hacker further access to the site backend, or to a particular user's account. When you enter logon information into sign-in fields, this information is typically converted to an SQL command. This command checks the data you've entered against the relevant table in the database. If your input data matches the data in the table, you're granted access, if not, you get the kind of error you would have seen when you put in a wrong password. An SQL injection is usually an additional command that when inserted into the web form, tries to change the content of the database to reflect a successful login. It can also be used to retrieve information such as credit card numbers or passwords from unprotected sites.

**Theft of FTP Passwords**

This is another very common way to tamper with web sites. FTP password hacking takes advantage of the fact that many webmasters store their website login information on their poorly protected PCs. The thief searches the victim's system for FTP login details, and then relays them to his own remote computer. He then logs into the web site via the remote computer and modifies the web pages as he or she pleases.

**Cross-site scripting**

Also known as XSS (formerly CSS, but renamed due to confusion with cascading style sheets), is a very easy way of circumventing a security system. Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack. In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed. Typically, attackers inject HTML, JavaScript, VBScript, ActiveX or Flash into a vulnerable application to deceive you and gather confidential information. If you want to protect your PC from malicious hackers, investing in a good firewall should be first and foremost. Hacking is done through a network, so it's very important to stay safe while using the internet.

**Presentation of the Findings**

**3. Introduction**

This chapter presents first, the organisations that use computers in Lusaka district; second the assessment on the relationship between the officers' qualifications and the use of computers in those organisations, third the evaluation on relationship between computer equipment and infrastructure available in the organisations.

The study seeks to achieve its general objective to assess cyber-crime and identify its effects in organizations and individual homes in Lusaka district. This study was necessitated by the researcher's interest to identify the ways to eradicate or reduce cybercrimes in Lusaka district of Zambia. The demand for use of ICTs by individuals and organisations both at national level and global in the contemporary world con not be over stated as it has become the order of all human tractions. organisations in Zambia for example no longer accept cash for organisation fees; they demand that customers deposit fees direct into organisations accounts. Not long from banks will stop handling cash as well since e-banking facilities are already available on the market. Hence the learning of ICTs by officers in organisations is no longer a luxury for few but a survival tool for the coming generation. It comes as a shock that in the communities we live in, people are not aware of the urgency for serious implementation of the Information Communication Technology policy and the ICT policy for basic education. The ICT policy for basic education was formulated to guide the integration of ICT way from kindergarten to secondary organisations and to higher learning institutions (Olatokun, W. M. (2009)) [3]. The goal of the study was to help communities to be conscious on the importance of cyber security education to inculcate in them a paradigm shift.

**Presentation of findings from officers**

**4.1 Gender of officers Respondents**

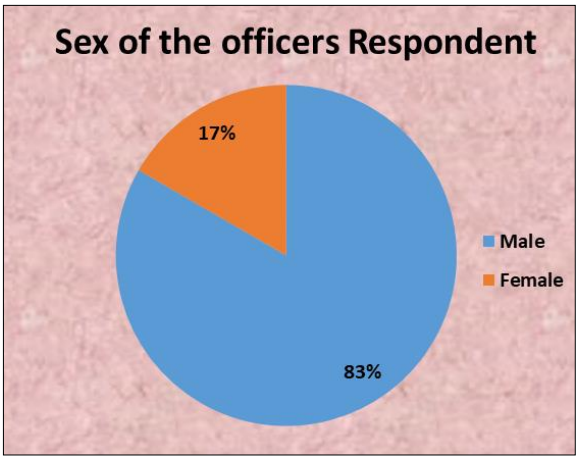


**Fig 1:** Source: Field Data, 2018

From the study of 100 Officers respondents, it indicates that they are more males than females. Figure 4.1 shows that (83 %) respondents were male and female respondents were (17%).

### 4.2 Trained in computer

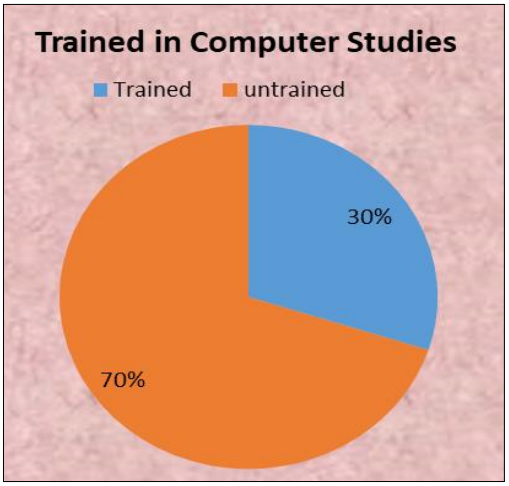


**Fig 2**

The study sought to find out the number of officers trained in ICT or computer studies who are assigned with responsibilities using ICT devices. The results presented in Figure 4.2 shows that 30% of the respondents were trained in ICT while 70%. Of the respondents were not trained but offered to use the computers.

The study sought to find out the competence skills officers had in using computers. The results are presented in table 4.1 and Figure 4.7 which expresses the percentages

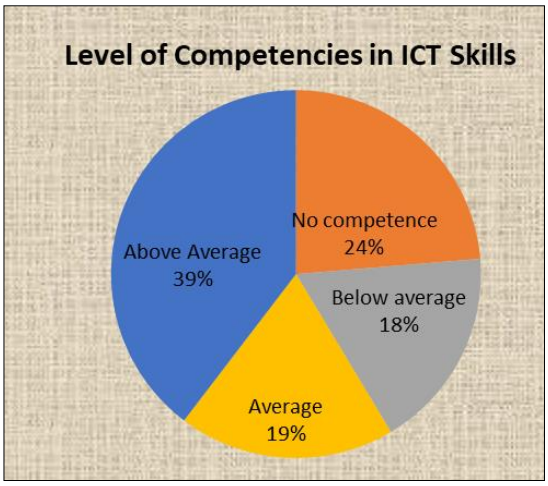


**Fig 3**

The research results from table 4.1 and figure 4.3 indicate that 39% of teacher respondent is advanced in skills like; typing, e-mailing, Texting, picture editing, Scanning, voice conferencing and many other skills in computer, 19% are average. 18% are beginners and 24% are unfamiliar.

### 4.4 Officers attitude in the use of ICT gadgets and the internet facility

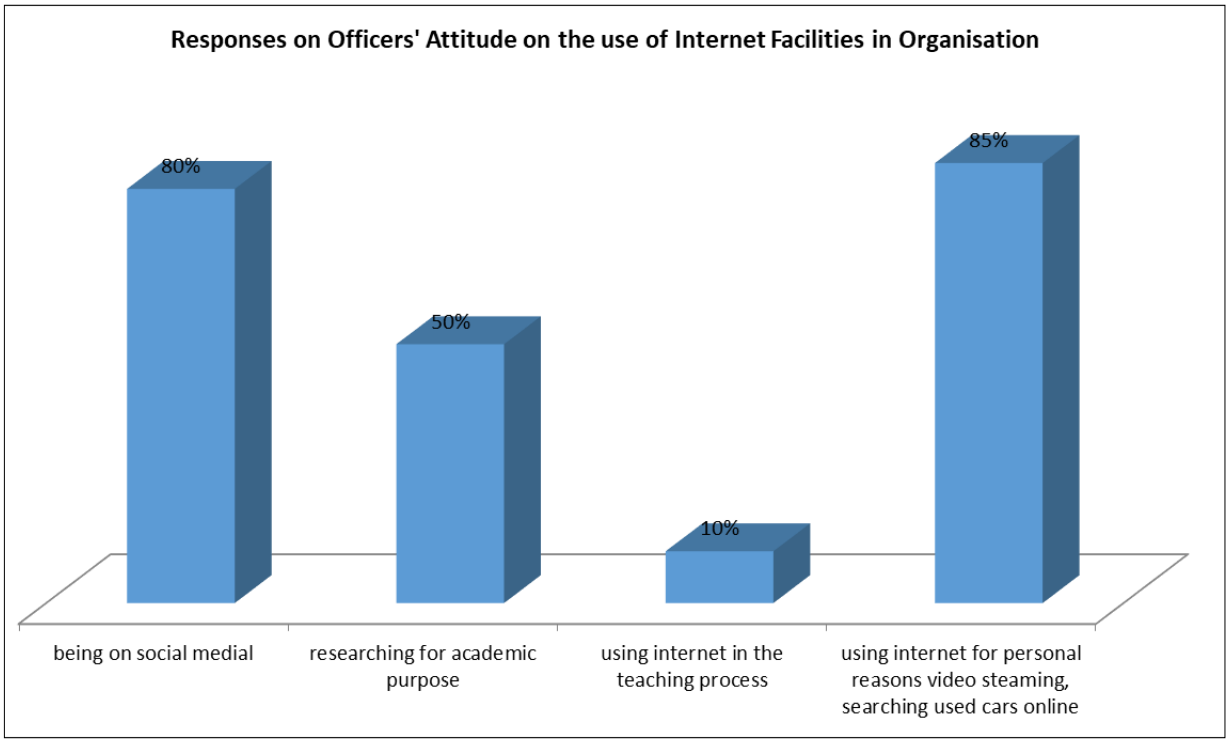


**Fig 4**

Effective using of the ICT devices comes with a number of emergent factors that may affect its effective working. Some of these factors include the officers' attitude on the use of the ICT facilities in organisations. Officers were asked for activities in which they mostly use the organisation ICT facilities and the results are presented in fig 4.4. 85% of the respondents indicated that the use the internet on personal activities such as video streaming and searching for used cars, 80% of the respondents indicated that the use it on social media while 50% of the respondents indicated that they use it for researching for academic purposes and only 10% use it for teaching process.

### 4.5 Identified Challenges in using ICT devices in organizations

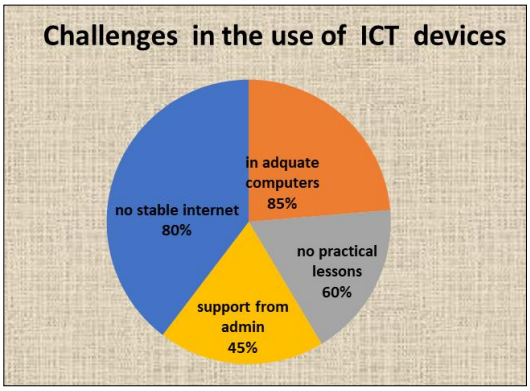


**Fig 5**

When asked for some of the challenges' faced by organization when using ICT devices in organisations, the respondents gave the responses as tabulated in fig 4.5. 85% Indicated that they face the challenge of inadequate computers to teach other officers while 80% of respondents indicated that their organisations have no stable internet connectivity. 45% of respondents indicated that the do get required support from their administration while 60% of the respondents indicated that they do not offer practical lessons as the number of officers outweigh the facilities available.

### 4.6 responses on the Managers personal experiences with cyber crimes

**Table 2**

| Respondent | Percentage |
|---|---|
| Managers agreed | 100% |
| Managers disagreed | 0% |

On the other hand respondents were asked if they themselves have been affected by cyber crime in their organisations. 100% agreed that they have been attacked before by cyber criminals.

### Presentation of finding from administrators on cyber security in their organisations

### 4.7 Responses from managers having some form of cyber security background

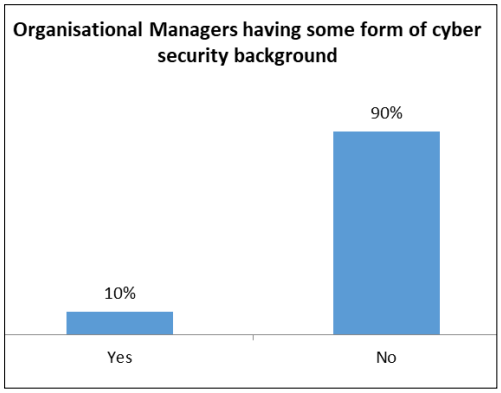


**Fig 6**

Fig 4.7 shows that 90% of administrators' respondents do not have any form of ICT background on 10%. This may negatively affect the cyber security in organizations.

### 4.8 Workers Responses ICT Facilities in organisations

The study sought to assess cyber security skills in organisations respondents to rate as a triangulation.

### Workers rating the quality of cyber security in organisations


**Fig 7: Sources: researcher, (2017)**

Fig 4.8 shows finding on the workers' rating of the quality of cyber security. The findings were that 7% rated above average, 60% rated average and 33% rated below average.

### Pupils' Response on have Facebook Account, WhatsApp Account, Email Account

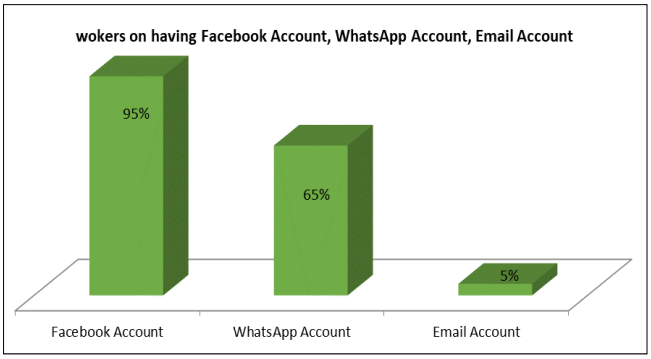


**Fig 8**

The researchers intended to find out whether workers in organisations have created their own Facebook, WhatsApp and e-mail accounts and to infer the results as a potential receipt for effective cyber security eradication. Fig 4.8 shows that 95% have Facebook account, 65% have WhatsApp accounts and only 5% have email accounts.

**Response of workers being allowed to own and use the ICT gadgets in organisations**

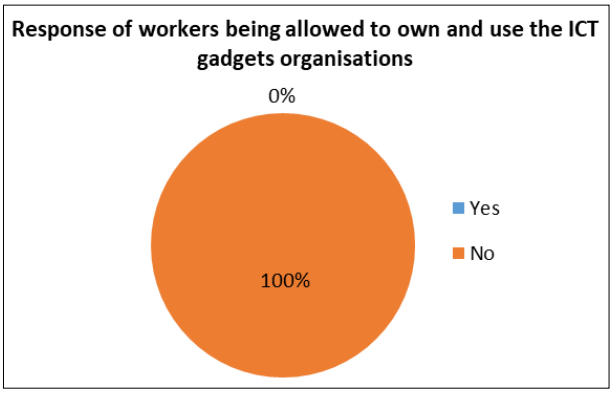


**Fig 9**

The researcher wanted to confirm with workers as to whether they are allowed to use ICT gadgets in organisations or not. Fig 4.9 presents results to this effect. 100% of respondents indicated that they are not allowed to own and use ICT gadgets in organisations.

**Data analysis and research discussion**

**4. Introduction**

This chapter presents discussion of the research findings as presented in chapter four. Discussions of the findings will be compared with literature that has been reviewed on the subject matter. It is important to note that emerging factors as the topic of the study presents are any situation that relates whether to the positive or negative contribution to the effective eradication of cyber security in Lusaka district were the study was conducted.

**4.1 Gender involvement in the cyber security**

The researching was aimed at finding out what emerging factors in the eradication of cyber crime in Lusaka district are affecting the effective eradication or reduction of cyber crimes. The researcher indented to find out the participation of gender in the cyber security and the results indicate that there is extremely low female participation in the cyber security in Lusaka district. These results are in agreement with report from the UNDP (2011) which indicate that girl child education is still a challenge in Zambia. The effective teaching of the subject means that all learners access the services and this can be enhanced if female workers get involved to stand as a model for the girl.

**4.2 Information and communication literace levels**

The results presented in fig 4.2 indicate that 70% of managers who work with computers in business institutions were not up to date in security systems studies. The results from this study are also in agreement with what Phiri and Silumbe, (2015) have noted, they indicate that a study of 22 organisations surveyed showed that 90% of the officers that teach ICT have not been taught how to teach the subject. The managers were hired to work because of their IT skills but without cyber security skills. Therefore, lack of knowledge regarding the use of Information, communication and technology (ICT) and a lack of skill on the tools and software have also limited the use of Information, communication and technology (ICT) tools in business organisations. Darbyshire, Philip (2000) [5] states that if there is lack of appropriate staff training and quality training for officers, the results will be very poor.

**4.3 Allowing workers own and use ICT related gadgets in business organisations**

ICT related gadgets are a brilliant aid in business organisations. Online business has revolutionized the business industry. Computer technology has made the dream of online business, a reality. Business is no longer limited to one nation but to the whole world. It has reached far and wide, thanks to computers. Physically distant locations have come closer due to Internet accessibility. So, even if buyers and officers are not in the same premises, they can very well communicate with one another and do business. There are many online businesses, whereby buyers are not required to attend to officers or be physically present for business.

**4.4 Reasons for not allowing officers to own and use ict gadgets in organisations**

Analyzing the reasons given to why officers must not be allowed to use ICT related gadgets in organisations are more of social complex than progressive. These reasons can effective resolved by any progressive minded administrator. Such factors are more human attitude than technical and logistical nature to continue affecting negatively cyber security. There will be need to learn from what other countries are doing in promoting the effective ways of using officers than dwell on none progressive opinions such as presented as reasons for not allowing officers own and use ICT gadgets in organisations.

**5. Recommendations**

Based on the results and findings of the research study, the following recommendations are hereby made:

- Institution managers and indeed all stakeholders in business organization should invest in cyber security.
- Government should include cyber security in the Ministry of education curriculum
- Cyber security should be taught in all organisations in Zambia.
- Officers should not be allowed to use personal ICT devices to do company jobs online.

**6. Conclusion**

Based on the findings above we suggest that the following ways that can be applied to reduce cybercrime. I am not saying eradicate cybercrime because this crime is evolving every day. So as I am writing this article one is already making new ways of doing his or her cybercrime. This will just help you not to be an easy target for cybercrime.

Use strong passwords: Use different user ID / password combinations for different accounts and avoid writing them down. Sichone C. (2011) [2]. "Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis". Do not share password: A password should never be shared with anyone in your family or place of work. Don't give it to your loved ones too. Don't write the password in your daily on anywhere else as doing so will make your data not safe to be hacked. Secure your computer by activating your firewall: Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of

viruses and hackers.

Use anti-virus/malware software: Prevent viruses from infecting your computer by installing and regularly updating anti-virus software. Be social-media savvy: Make sure your social networking profiles (e.g. Facebook, Twitter, YouTube, Google+, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever! Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location. Secure your wireless network. Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

Avoid being scammed: Always think before you click on a link or file of unknown origin. Don't click on the links in these messages as they may take you to a fraudulent, malicious websites and don't feel pressured by any emails. Motah M. (2008) [4] "Check the source of the message". Legitimate companies will not use email messages to ask for your personal information. When in doubt, verify the source (e.g. contact the company by phone). Never reply to emails that ask you to verify your information or confirm your user or password.

## 7. References


1. Phiri W, Mbobola A. Emerging e-learning technologies and Zambian education system: A focus on rural areas, 2018, 216–221.
2. Sichone C. 'ZICTA Responds to School ICT Curricula Challenges'. *Times of Zambia,* 2011, 9. www.zicta.zm/2018 Zambia Information and Communications Technology Authority Survey preliminary Report.pdf; accessed 22:05-02/06/2020
3. Olatokun WM. Issues in Informing Science & Information Technology, 2009.
4. Motah M. Issues in Informing Science & Information Technology; The Social Cost of the Integration of Information and Communication Technologies, Information and Communication Technologies, Information, Education and Communication, on the Young of Republic of Mauritius, 2008.
5. Darbyshire, Philip. User-friendliness of computerized information systems. Computers in nursing. 2000; 18:93-9.