An Assessment of Some Dangers Associated with the Use of Pirated Software on Computers

Abdullahi Ayegba[1], Hayatu Idris Bulama[2], Oyekunle Oluwatoyin Victoria[3], Idris Shehu[4], Adejoh Joshua[5], Omakoji Odiba[6], Oyibo David[7]

[1]Cyber Security and Privacy Unit- NACES, Engineering and Space Systems Department, National Space Research and Development Agency, Abuja, Nigeria

[2]Department of Electronical/Electronics Engineering, Airforce Institute of Technology, Kaduna State, Nigeria

[3]Computer Science Department, Federal Polytechnic of Oil and Gas, Bonny, Rivers State, Nigeria

[4]Strategic Space Application Department, National Space Research and Development Agency, Abuja, Nigeria

[5]Mathson Research Consult, Mathson Space International School, Abuja, Nigeria

[6]IT Consulting, Infosys Limited, United Staes of America

[7]GeoApps Plus Department, National Space Research and Development Agency, Abuja, Nigeria

ABSTRACT

The aim of this research work was to investigate some dangers or risks associated with the use of pirated software on computers. The research made use of descriptive analysis of qualitative research method. From the results, it was concluded that there are several dangers and risks associated with the use of pirated or unlicensed software such as discouragement and "killing" of software industries, no software updates available for pirated software, virus attack, document loss, legal action against the users, etc. It was recommended that adequate sensitization be made in different organizations by the management either in a form of seminar or a group discussion on these risks or dangers of using pirated software in order to avoid any of these risks sooner or later. It was also recommended that future research works be done on the factors responsible for the use of pirated software in the society with a view to finding some possible solutions.

KEYWORDS: Attack, Breach, Dangers, Piracy, Software, Virus, Unlicensed

1. INTRODUCTION

A software is a set of instructions or progarmmes installed on a computer, and used for the operation of the computer as well as to execute or carry out various tasks. The use of software is highly connected with cyber security as cyber-attack can occur through the use of particular software, especially those not legally obtained or installed.

Cyber security is defined as the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access. It is also defined as the protection of Internet-connected systems, including hardware, software, and data from cyberattacks (Adamu *et al.,* 2022).

Piracy is defined as an unauthorised use or reproduction of another person's work. Piracy can also be defined as an unauthorized duplication of someone's copyrighted content which is then sold at lower or lesser price. This copyrighted item or content can be written articles, books, film, recording, patented material, television programme, etc. Pirated software is the software that has been duplicated or reproduced without authorization, and sold to the people at any price. Software piracy is simply put as

any unlawful distribution, or use of software. It is such a "lucrative business" that has lured organized crime groups in a number of countries. Software piracy rate was reported to have been 36% by the BSA. On the other hand, Copyright is a legal means of protecting an author's work (David, 2020).

In the society today, many people prefer a cheaper commodity without considering the consequences that may follow after buying such an item or material. That was how the people pirating other people's works were able to have the people patronizing them including some who may be aware of the consequences of using such products.

Over the past years, the world has seen rapid growth and great achievements in the field of information technology. This has resulted in the expansion and rapid progression of the software companies. As the software companies have expanded in huge numbers, so has the criminal activity of software piracy (Ishwor, 2015).

It follows that the best strategy for software firms would be to increase the protection level as much as possible so that potential pirates would simply find it very costly to pirate. But according to Conner and Rumelt (1991), by taking into account the effect of network externalities, as commonly found in software products, a high level of protection may not be optimal for firms. They added that in a monopoly setting, raising software protection would be profit maximizing only when there is only insignificant effect of network externalities. Otherwise, profit would decrease with an increased protection level because some would-be pirates are forced to do without the software, rather than buying it (Samuel, *et al*, 2006). Software piracy is a crime commonly defined as illegal copying, downloading, sharing, selling or installing of copyrighted software. The majority of software today is purchased as a single-user license, which means that it can be used by one authorized user in one or more machines as long as the same licensee is the only user. However, making multiple copies of it and sharing it with friends or relatives or for commercial purposes is considered to be violation of the license terms and conditions (Ishwor, 2015).

With the continuous decline in the level of social and economic well-being of people in various communities in Nigeria; there have been series of crime, ranging from cybercrimes and social distortion to other forms of robbery. One of such criminal acts with a viral prevalence is the act of software piracy which is also known as illegal copyright infringement of software (Schmuhl, 2019). Although the government has put in a lot of resources to curb the escalation of piracy in Nigeria, the pace of internet fraud and software piracy has increased overtime in Nigeria (David, 2020).

According to Federal Bureau of Investigation, USA (2013), in order to buy a software legally and use it legitimately, some of the tips are: When buying a computer, one should always ask for a genuine, pre-installed operating system, and then check out the software package to make sure it looks authentic. Also, purchase all software from an authorized retailer. And if one is not sure which retailers are authorized, he or she should visit the company website of the product of interest. In addition, check out the company's website to become familiar with the packaging of the software you want to buy. Be especially careful when downloading software from the Internet, an increasingly popular source of pirated software. Purchase from reputable websites.

These have to be followed or adhered to because, whenever, a person installs and use unlicensed illegal copy of certain proprietary software, it's considered software piracy no matter how they get it, whether it's being downloaded from the internet, transferred from friends or bought it illegally. With the demand to complement daily productivity, students and information professionals are the group that potentially, highly and easily been influenced to use pirated software (Loch & Conger, 1996; Mastura, Thurasamy & Tee, 2008; Haque, Rahman & Khatibi, 2010 and Anwar, Bahry & Amran, 2012, Norizan *et al.,* 2015). As a result of the continuous rise in the use of the pirated software in the society or some parts of the world, as reported in some works above even as there are laws for curbing it, there is a need for further study of the dangers that are likely to occur when one is using pirated software on his or her computer, thus, the need for this work.

2. METHODOLOGY
This research work makes use of descriptive type of qualitative research method. The descriptive method of qualitative research approach used for the work was to allow adequate explanation of each item or danger that can result from the use of pirated software. A descriptive research design can use a wide variety of research methods to investigate one or more variables. Descriptive research aims to accurately and systematically describe a population, situation or phenomenon. The data used in this research work were secondary data which comprise the library and internet materials.

3. RESULTS AND DISCUSSION
Research question: What are the dangers associated with the use of pirated software on computing devices?

The following enumerates some of the identified risks of pirated software:

1. **The use of pirated software leads to discouragement and "killing" of software industries:** Before an application or software is produced, a lot of efforts have been put in. In some cases, this is done to improve on the exhibiting one, especially to address the challenges or setback of the existing one as obtained through user feedback. And in some cases, completely new software is developed where the core elements of the existing version cannot support new feature requirements of industrial trends. This is done by the industry in order to make their money while also meeting the needs of the users. However, pirates may start to acquire the software illegally even after few days of its release without buying it from the owners. As a business person, there is no way one will not incur losses after spending months on the work and at the end one has little or nothing from it. Consequently, the industry may not plan to go into another research or to develop another software again. In fact, the owner may even close down the industry especially if there is no fund to pay the staff members of the industry. One, as a person using the pirated software instead of buying has contributed to the "killing" or closing down of that business. He or she has refused to appreciate the software industry's efforts to create quality software, and has deprived them of their rightful revenue. Even in Nigeria, this is happening in other areas or products apart from software. Film industries are suffering the same thing. For instance, the film produced today which are sold at the designated stores for N5000 may be seen tomorrow or after some days in a wheelbarrow and it will be sold at N500. Drinks, foods, and even drugs are affected by this adulteration and piracy. The original owners are always the ones losing.

2. **The use of pirated software also lowers one's level or standard in a higher technical gathering:** This can come up when a discussion is going on in a practical training, and each participant is being asked of the software they are using. The person can still go further to ask how much each person bought his or her own. This training might also have in attendance some of the software industrial owners, probably being part of the guest speakers or sponsors or promoters of the event. Now, imagine many people tell how much they bought their own software, and how long their license would last only for one to respond that a computer or cybercafé owner in on a particular street installed it for him or her. He or she only paid the person … and he or she will call an amount which is not even up to one-tenth of the amount others said they bought their own software. Automatically, image of the person using the pirated software has been altered or reduced in the gathering. He or she will not be comfortable throughout the programme. The other participants would also see him or her in a different way from the earlier time this discovery about him or her was not made. He or she may not even be invited to such an event next time, because you are one of those who are destroying what they are building in society. It may even cut his or her ties with other top colleagues because of his or her "selfishness" and lack of support for others to grow.

3. **No Updates available for pirated software:** If one is using a licensed software, as soon as the industry updates their software, the updated one will be available on the website for the users to use in updating their older version of the software. In some cases, the users are even sent an email to click on a link sent to their email to update their software. This is not available to those using pirated software. Software is updated by the industry in order to meet up with emerging or new challenges in the society. As the problems are being discovered, the solutions are also being provided, and this will be added to the features of the existing software. These new features can only be available in the newly updated software, and can be accessible by the existing people or users with legitimate software or with license as well new users that will buy software legally after the update. Users of pirated version cannot update theirs, and will be incapacitated in a way because it is not all the works or tasks that their software can do unlike those with license. In fact, trying to update the pirated software will make some of them to be totally crashed and stop working because the owner will automatically detect it. That is why when some people are making use of some applications, or computer software, they will never connect their computer to the internet because even without going to "update the software", it connects itself automatically to the owner's website, and in the process get detected and crashed automatically in the computer. Some GIS software do that, from my investigation.

4. **It leads to Virus or malware attack:** Some of the pirated software are downloaded from the websites of other people or pirates other than the

owner. Some of these websites are well secured or protected against viruses. When this software is being downloaded with virus already in it, and installed on the computer, the computer is already infected with a virus. All the documents or materials on the computer will be affected. Some software are even copied from the computer already infected with virus. It is like copying a document from a virus-infected computer in a flash to another computer. As soon as the flash is being inserted into the other computer, it will display that a virus has being detected. If the computer does not have a strong and updated anti-virus software, then, it will be affected and the documents or works in it will all be affected or even lost. This is just copying of document let alone installing the virus-infected software on the computer. It has deeply gone into all the parts of the computer, and would result in losses immediately, sooner or later.

5. **It can lead to software instability and document loss:** When one is using pirated software, the software does not have the capacity to do some things or perform some tasks. This is because, it does don't have the feature which will enable it to perform those tasks. Some licenses are for one year or for a timeframe. It has a stipulated number of users too. In the case of pirated software, it is like forever, there is no expiry date, there is no maximum number of users, etc., and this made it to have a limited capacity. From investigation, it has been revealed that some computers even shut down when using the pirated software to perform some tasks which are probably higher than it can handle. This can be disastrous especially if the processes passed through during the simulation or design or processing before arriving at the point it crashed or shut down were long and tedious. This is simply loss of document or work, and it cannot happen when one is using a licensed software because the user can take a legal action against the company for the damage or loss caused. So, some mechanisms to prevent such incidences are put in place as part of the features of the software. This can happen even if it is a PhD final work or financial report or any important work. It can even happen that apart from design or processing, the work being done can refuse to save until the programme is closed or the computer is being re-started. In the process of re-starting the computer, many of the works or corrections made in the work will be lost, and one would have to start all over again. This is a

great danger, and it is because of the use of pirated software.

6. **The use of pirated software can lead to a legal action against the user:** In a simple term, it can be seen as property theft. It is like a commodity being displayed in a market, but instead of buying it, one goes there to cut part of it to use. In Nigeria, it is a criminal offence to use a pirated version of someone's software or other items. This is an illegal use of someone's property or to be in possession of someone's property illegally and without following due process. You, as a user, is causing damage to the owner or seller of the software. And since, the pirated software is being acquired and used as a "stolen" item, the user, when caught, will be treated as one who stole other person's property. In other words, a legal action can be taken against the user, and he or she will pay severely. For instance, in September 2012, the federal high court Abuja sentenced an accused person of copyright infringement to three months imprisonment and a fine of N12,600 (Nigeria Copyright act and piracy, https://omaplex.com.ng, Sept 7, 2012). In other words, it can result to legal consequences, which will include fines and criminal charges by the owner against the users of the pirated software.

7. **Pirated software has performance problems:** In any computer work, one of the things needed is speed. Another is efficiency, i.e., to work effectively. A situation where the computer keeps hanging or freezing from time to time, resulting in shutting down of computer, slows down work. In the case of large data processing, pirated software cannot perform such roles, and even if it is doing it, it does perform effectively like the licensed one. It can result to slowing down of computer operation, computer delay as well as freezing of computer during work which will make the system not to respond to any command.

8. **It can lead to personal information loss or being stolen:** Some pirating agents or pirates add some codes in the pirated software, and when this software is being downloaded and installed on a computer, it has the capability to extract some information from the computer. This will later result in information leak or even loss no matter how delicate or restricted or classified the information is. That is why account section of any organization should never use unlicensed or pirated software. Examination bodies or even industries involving in design and manufacturing are not to use pirated software too because it can

used to extract their information secretly, and have them transformed into theirs or use them for other purposes including asking them for payment before they release them back to the owners. This can be referred to as hacking. It can result in phishing too. Phishing is the process in which someone obtained the personal information such as names, addresses and security number or even password of another person. With these details, the person can now be acting as the real owner and, then be defrauding people especially those who are closer to the original owner of the details. In fact, aside these people or bodies, nobody should use pirated software.

4. CONCLUSION

The research work on the dangers associated with the use of pirated software on computers or computing devices has carried out using descriptive analysis of qualitative research method. From the results, it can be concluded that there are numerous dangers associated with the use of pirated or unlicensed software on computers, and some of them are discouragement and "killing" of software industries, no software updates available for pirated software, virus attack, document loss, legal action against the users, etc.

5. RECOMMENDATION

It is recommended that adequate sensitization be made in different organizations either in the form of seminar or group discussion on the risks or dangers of using pirated software in order not to be found wanting of any of these dangers or their combination. We also recommend that future research works be carried out on the factors responsible for the use of pirated software in our society or some parts of the world with a view to finding some possible solutions.

6. REFERENCES

[1] Anwar, N., Bahry, F. D. S., & Amran, N. (2012): Installation and Use of Pirated Software: The Factors Behind It. *Proceeding of Business, Engineering and Industrial Applications (ISBEIA),* 207-212.

[2] Adamu Abdullahi Garba, Maheyzah Muhamad Siraj, Siti Hajar Othman (2021): "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria". International Journal of Electrical and Computer Engineering. Vol. 12, No. 1, pp. 572-584

[3] Combating Software and Hardware Piracy; (2016). Available at https://www.academicwritersbure au.com/samples/220-combating-softwareand-hardware-piracy

[4] Conner, K.R. and Rumelt, R.P. (1991): Software Piracy: An Analysis of Protection Strategies, Management Science, Vol. 37 (2*)*, pp. 125-139.

[5] Haque, A., Rahman, S., & Khatibi, A. (2010): Factors Influencing Consumer Ethical Decision Making of Purchasing Pirated Software: Structural Equation Modeling on Malaysian Consumer. Journal of International Business Ethics, *3*(1), 30-40.

[6] Ishwor Khadka (2015): Software piracy: A study of causes, effects and preventive measures. B. Eng Thesis, Helsinki Metopolia University of applied science.

[7] Federal Bureau of investigation (2013): Consumer Alert: Pirated Software May Contain Malware.

[8] Kwan Samuel, Jaisingh Jeevan and Tam Kar Yan (2006): Risk of Using Pirated Software and its Impact on Software Protection Strategies, *PACIS Proceedings*. 35. http://aisel.aisnet.org/pacis2006/35

[9] Loch, K. D., and Conger, S. (1996). Evaluating Ethical Decision Making and Computer Use. *Communications of the ACM, 7*(39), 74-83. http://dx.doi.org/10.1145/233977.233999

[10] Mastura, J., Thurasamy, R., & Tee, W. T. (2008): The Intention to Use Pirated Software: A Study of Undergraduate Students in a Public Institution of Higher Learning in Malaysia. *Problems and Perspectives in Management*, *6*(2), 4-12.

[11] Nigeria Copyright act and piracy, https://omaplex.com.ng, Sept 7, 2012

[12] Norizan Anwar, Mohd Mursyiddin Abdul Manaf, Noraizan Amran, Farrah Diana Saiful Bahry (2015): The Use of Pirated Software among Information Professionals: Measuring the Difference. Journal of Management Research. Vol. 7, No. 2, pp 353 – 363.

[13] Schmuhl MA, Na C (2019). Globalization and software piracy within and across 103 countries. Crime, Law and Social Change. Vol 72(3):249-67.