

**ESTABLISHMENT OF A CYBER CRIME DEPARTMENT IN
UGANDA POLICE**

**COMPILED BY D/C ASP MUGISHA GREGORY
20/05/2009**

1.0.

INTRODUCTION

Computers are being used extensively in all sectors of the Uganda economy. They are used in the private and public sectors/commercial and non-commercial sectors/service and non-service sectors/academic and non-academic sectors such as Banking, agricultural, Industrial, Police, Military, Scientific Research, Health and other Governmental Agencies because they do not only facilitate fast functioning of the organization but also store vital information, which is a very valuable commodity. In addition to the computer growth in the Uganda economy, they have been increased growth in the information technology (IT) especially the mobile revolution. This has given birth to a new e-culture in Uganda, which is being characterized by eBanking and ePayment to some extent and soon Uganda will follow the developed countries to, eLearning, ePassport, eImmigration and so forth and these will continue to bring technology to the doorsteps of many like never before. Thus, digitalization is fast becoming a way of life with the Ugandan people.

Though technology brings growth and development, it also enables fraudulent practices, which has been referred to **cyber crime** or **computer crime**, **e-crime**, **hi-tech crime** or **electronic crime**. These terms generally refer to criminal activity where a computer or network is the source, tool, target, or place of a crime. These categories are not exclusive and many activities can be characterized as falling in one or more. Additionally, although the terms computer crime and cyber crime are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. As the use of computers has grown, computer crime has become more important.

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), electronic fraud, intellectual property infringement, hacking, industrial espionage, on-line child exploitation, Internet usage policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more.

The consequences of computer crimes are or will be enormous in Uganda as it has been elsewhere with increasing computer and IT usage. Florence Tushabe and Venansius Baryamureeba (2005) conducted a study in relation to cyber crime in Uganda, which shades some light on the situation. The study revealed that in January 2005, a multi-million dollar scam involving a fraudulent intranet bank transfer between Standard Chartered Bank, Nairobi and Barclays Bank, Kampala was unveiled. A prominent Ugandan businessman and construction magnet together with two Congolese nationals were wanted by Interpol (Kenya) over accusations of

masterminding the bank fraud that saw Kenyan Standard Chartered Bank staff wiring to them \$5 million in three installments to separate bank accounts and recipients in Kampala. In July 2004, one lady lost her passport and 500 dollars (which she had borrowed) to a fake company claiming to arrange visas and free transport and accommodation in Canada. They used an existing project by the Ministry of Health in which some officials were to travel to Toronto for a Trainer of Trainers (ToT) course in HIV/AIDS management. She thought it was a genuine deal when she saw a website on the Internet containing the details of the conference. On the day, the passports (including the visas) were to arrive, the perpetrators of this scheme disappeared. Several others fell victim of this scam and similar ones.

One company confessed about an incident of email spoofing in which a supposed employee sent an email to their clients threatening that the aircraft they were using for business was in poor condition and passengers should use it at their own risk. Many passengers began canceling their flights for no apparent good reason. The company sought an IT specialist and together with their system Administrator, carried out the investigation, which traced the bad email to an employee in a competitors company. The case was settled out of court In July 2004. According to an estimate made by "business week" in 1990 the total loss due to computer related crimes alone was in the range of 3 to 5 billion dollars and as on date the lose could be many folds of the sum.

The new vision newspaper broke a story about two pornographic sites, www.kimansulo.com and www.hotugandans.com hosted in Canada but selling thousands of pictures and videos of Ugandan women having sex. A follow-up story by a journalist from The Monitor newspaper said, "But most of the 'models' in the thousands of nude pictures on kimansulo.com are not actors and many did not know that their pictures were taken while having sex. They were ordinary office workers and university students who go for a party, get drunk and end up having a fling with someone they thought was a friend. Unknown to them, a concealed video camera is rolling away, recording the minutest details of their actions and facial expressions". By the end of August 2005, they had closed their websites due to public outcry.

Generalized results of Florence Tushabe and Venansius Baryamureeba's (2005) study show that over 90% of the people who participated in the study reported to have been a victim of at least one cyber crime incident and twenty-five percent confessed that they committed at least one wrongful act while in the cyberspace. The victims were mainly prey of SPAM, virus attacks and pornography, while the perpetrators are mostly SPAM senders, intellectual property infringers and hackers.

Thus the need to set up a cyber crime department in Uganda Police is that although IT promotes convenience, it is this very characteristic that is being used to aid and abet crime today. Criminals no longer need to be at a crime scene, but can perpetrate crime especially through the cyberspace from anywhere at anytime. Technological advancement has opened the door for the bad and ugly to come in and undesirable elements now take advantage of the digital culture to do harm to the unwary. Children can no longer safely surf the net because of the danger it poses to the unsuspecting. Businesses have to be careful to secure their business

and even government bodies as well are not left out and critical data can be compromised at the drop of a hat.

Any sabotage to the system or destruction of data, software and hardware would result in a great financial loss to the concerned organizations. Thus, on the one hand the computers have not been proved to be an advantage to the humankind but have also become a potential and safe cracking tool in the hands of criminals on the other who compromise the efficient and effective functioning of the organizations. They could perpetrate not only their traditional activities with greater ease and impunity, but also usher in a new crime and created new targets.

The dimension and volume of computer crime cannot be estimated precisely because very few people permit leakage or crime committed in their organization. This is due to the fear of losing customer's confidence or affecting employer's morale, both of which would lead to a drop in the business of the organization. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. The advance in computer technology is so that the gap between computer technology and security technology is widening day by day. The problem is further compounded by lack of awareness in the new kind of crime.

In all, this shows that the public is not protected against these kinds of crimes and their consequences. On this backdrop, it is high time that we address ourselves to meet the new challenge by developing deep insight into various aspect of computer crime, and evolve new investigative skills to meet the specific standard of legal proof. Some steps have been initiated such as a Contingent of five Ugandans from different offices in CID Directorate with different professions who selected and sent to Mubarak Police Academy (Cairo-Egypt) and empowered with the necessary skills and techniques/expertise to comb cyber crime. Individual/Personal Security, International Terrorism, Organized Crime, Cyber Crime, E-fraud, Citizens Privacy, State Security visa vis E-crime, Intellectual Property Crime were among the topics, which were covered. However, more need to be done to effectively curb this crime in the country.

2.0. WHO COMMITS A COMPUTER CRIME?

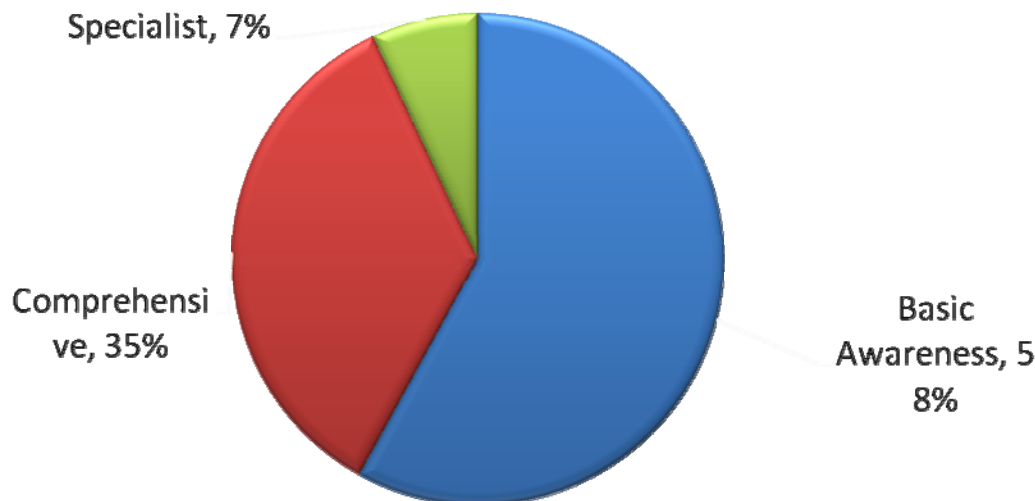
Many computer related crimes are opportunistic in nature. The perpetrators of computer crime in an organization can be either insider or outsider working alone or as a team possibly collusion in with insiders and outsider

- Employees of the organization.
- Employees of the organization (some employees handling computers consistently coming before and office timings without reason).
- Disgruntled and discharged employees.
- Employees handling sensitive information.
- Employees who are transferred out of police coming back seeking information about new passwords and codes

- Competitors or rival organization.
- Organized criminals including terrorists.
- Juveniles/Teenagers.
- Students.
- Individual spies
- Criminals
- Foreign Government

3.0. TECHNICAL COMPUTER AWARENESS LEVELS IN THE WORLD:

Computer awareness is broadly subdivided into three Levels i.e. Basic Awareness (58%), Comprehensive (35%) and Specialist (7%) as illustrated in the pie chart below:



4.0. COMMON TARGETS OF COMPUTER CRIME AND OPPORTUNITIES THEREOF

Now the information on the computer is treated as intellectual property, which is even recognized by courts. So this is also kind of property is subject to theft and cheating.

- Business houses may be targeted by their competitors.
 - Banks and other financial institution may be targeted by professional white-collar criminals.
 - Any commercial, industrial or trading company may be target of its employees or ex-employees of competitors.
 - Any organization of government or service industry may be the target of terrorists.
 - Military and intelligence may be targeted by espionage agents
 - Universities, scientific organization, research institutes may be the targets of students, industrial or business houses and other anti-social elements.
- Besides the above targets any computer user may be a target of "hackers" and "crackers" or "freakers" who do it either for intellectual challenge, for revenge, for gain or for fun.

5.0. MOTIVES OF CRIMINALS

Very often people committing computer crimes had any one or any combination of the following motives:

1. Personal/financial gain
2. Adventurism
3. Entertainment/fun
4. Revenge
5. Vandalism.
6. Intellectual curiosity
7. Political/ideological
8. Accidental.

6.0. CLASSIFICATION OF COMPUTER CRIMES

Computer crimes can be broadly classified as cases where 1–computer itself is the target of the fraud 2- where computers used to commit fraud, and 3- where compute is only incidental to other crimes.

6.1. COMPUTER AS A TARGET OF CRIMES

- Sabotage of computers, system or computer network.
- Sabotage of operating systems or programmes.
- Theft of data/information e. g marketing information.
- Theft of computer software [intellectual property.
- Blackmail based on information gained from computerized files such medical information, personal history sexual preference, financial data etc.
- Unlawful access to criminal justice and other government records.

All the above crimes involve Techno-Tress pass and unauthorized access to computer systems and data or programmes stored in computers .In such cases the intruder only looks at a file and even this violates owner's privacy.

6.2. Computer assisted crimes

- ATM [Automated teller machine fraud]
- Credit card fraud
- Frauds manipulated computerized bank accounts
- Tele-communication fraud.
- Frauds relating to electronic commerce and electronic inter-charge [EDI].
- Counterfeiting.
- Software piracy.

6.3. Computer incidental to other crimes.

In this category of computer crime, a computer is not necessary for the crime to occur, but is related to the crime act. This means that the crime could occur without the technology. However, computerization helps the crime to occur. Such crime include money laundering unlawful banking transaction, bulletin board system [BBS], supporting organized crimes records, computer aided murder, UNABOMBO cases of USA ,cyber terrorism and extortion through internet.

6.4. Probable penetration points

The vulnerability of crime could be

6.4.1. Hardware

Basic computer terminals, printers modem storage media and other peripherals.

6.4.2. Software

Operating systems and application programmes, most of the attacks are on proprietary and menu driven application programmes, which are meant for performing business operations such as accounting, inventory, billing etc.

6.4.3. Communicaton

Connecting a computer to any kind of network increases the vulnerability of the information stored on it. Therefore, the internet and other large international interconnection networks pose a special problem.

7.0. MODUS OPERANDI OF THE COMPUTER CRIME

Digital or electronic trespassing requires very few tools such as home computer, which be a note book computer and or desktop personal computer, a modem and a telephone line. The criminal first identifies and breaks into communication channel to which the computer is connected to the public data system network. He then tries to log into the system by trying various passwords. It is possible that he might have stolen the passwords. For an insider to gain unauthorized access to the system becomes easier. In the case of standalone systems, his job becomes easy once he gets physical access to the system

7.1. Telephone freaking:

It involves manipulation of telephone system by electronic trickery. Criminals take long distance telephone calls by avoiding payments for these bills. After dialing a number, pressing the proper sequence of keys before the telephone is answered would disconnect the call at the same time keeping the line open. After this, any number dialed would be seen as origination not from the freaker's own number at the other end of the open line to which the call is billed.

7.2 Computer machine:

It involves decoding of password breaking into the system and unauthorized use of system. Electronic eaves dropping could also be used as method by hackers for interception of computer service.

This is always done by Password cracking. Through this means they easiest way is to use programs specialized in cracking passwords, which can be obtained easily.

Example of three computer sets linked together by a hub

7.2.1. Interior violation:

Victim
PC (Win)



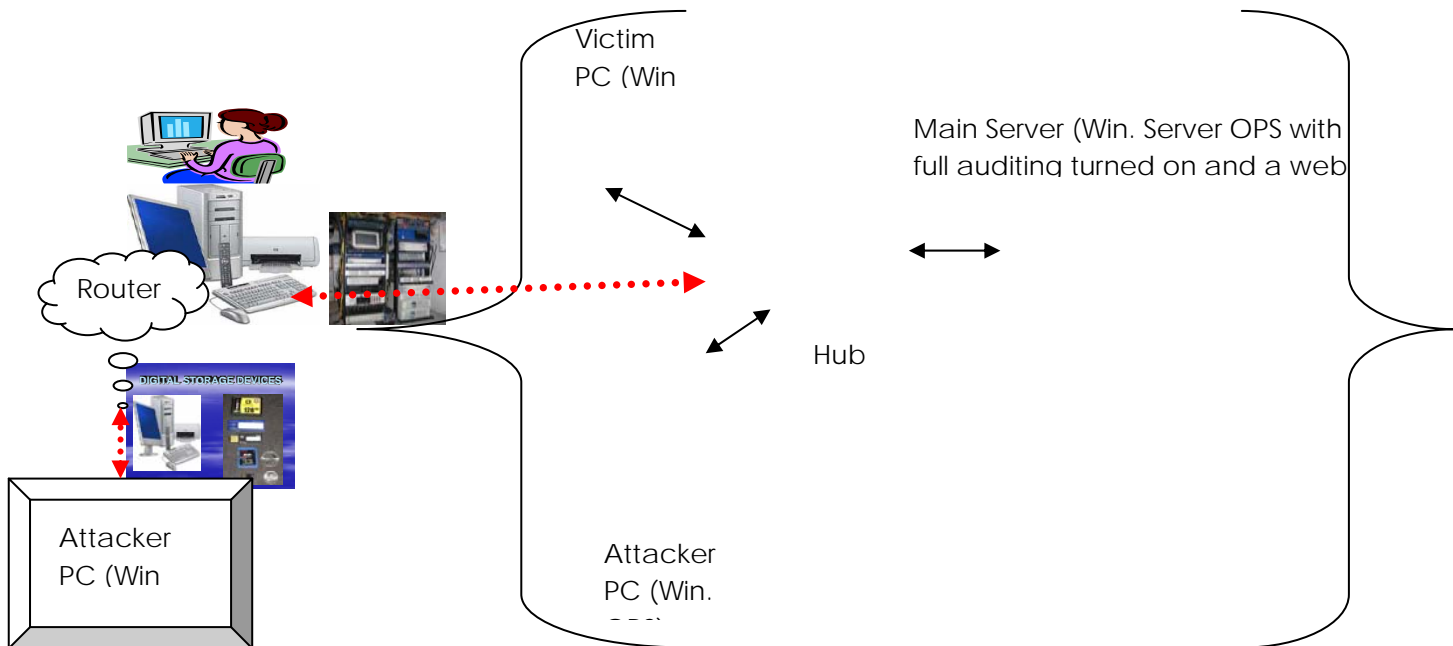
Hub



Main Server (Win. Server OPS with full auditing turned on and a web

Attacker PC
(Win. OPS)

7.2.2. External violation:



Advice:

- To use pass words with both characteristics for example letters and figures.
- System administration should be aware and should be ready all files. He uses the intrusion Detection programs assigned for identifying violation on the system.
- Take care of log file and the Fire walls

8.0. VIRUS:

Virus is a program inserted to other program and spreads it from one system to another. It can spread to other computers when the affected programmes are copied.

A Virus is a program code, its main function is to change or destroy information inside another computer. It has the ability to link itself to other programs on your personal computer or network. Viruses can be sent through Emails, They can also be transferred through other communication devices. Viruses can be generally divided into groups.

8.0.1 Parasite virus

It attaches itself to other programs and gets activated when the program is activated. It spreads to other programs and gets activated more and more. It spreads to other computers when any program of the infected computer is copied. There are two known parasite virus, Jerusalem and data crime.

- Do not allow outside floppy to be used in your computer.

- Avoid playing computer games on a computer where important data is stored. Virus spread faster through games.
- If virus is detected, immediately take step to defect it. Do not use a
- Keep all original EXE & COM files in a write-protected floppy.
- These floppy are to be copied in other PC. Then only from right protect original floppy
- Check for the virus. When the floppy hangs or refuse to react to your command.

8.0.2. Anti-virus vaccine

Computer virus and virus cause human diseases have the similar nature.

The computer viruses cause the computer to suffer whereas human viruses cause human beings to suffer. For both there is a vaccination.

Whenever computer viruses are detected, you have to see this Anti-Virus Vaccination like DR Solomon, Norton Anti Virus etc. These are also nothing but cleverly designed program to kill viruses.

However, you should remember that certain types of virus are difficult to remove. The damaged files will be lost forever unless you have a backup.

8.03 Specific problems created by viruses include:

- ♣ Filling disc or memory with unusable information (i.e. garbage).
- ♣ Altering files.
- ♣ Changing the File Allocation Table (FAT) in a personal computer so that files cannot be located.
- ♣ Changing the boot sector so that the computer will not run.
- ♣ Initiating or formatting the disc so that all information is destroyed.
- ♣ Changing the key stroke definition table.
- ♣ Licking the keyboard
- ♣ Altering the programs files.
- ♣ Printing or displaying inappropriate messages.
- ♣ Slowing program execution time.

ADVICES:

- Advisable to have checking rooms.
- Spying programs.
- Desist from singing into obscene sites.
- Not to open internets from unknown sources.
- Antivirus should be up dated.

9.0. TECHNIQUES OF COMMITTING COMPUTER CRIME

Techniques of committing computer crime could be data related or simply physical:

- 9.1. Sabotage:** Physical or logical damage to computer program or data by use of any liquid, gas ,fire, projectile, electro-magnet shocks or by living organisms. It also includes physical breakage of the computer or peripheries or damage of them.

- 9.2. **Eavesdropping and spying:** Wire tapping and monitoring radio frequency emanations are kept in this category. A criminal is in position to unauthorized signal on a communication line or data channel.
- 9.3. **Scanning:** This is the process of preventing squently-changed information to an automated system to identify those items that receives a positive response from computer. This method is used to identify telephone numbers that access computer users Ids and pass word that facilitates access to computers as well as credit cards numbers that can be used illegally for ordering merchandise or services through telemarketing.
- 9.4. **Impersonation:** In this process, one person assumes the identity of authorized users by acquiring identification items such as metal keys, stripe cards knowledge [pass word] characteristic [facial characteristics hand geometry, voice

9.5. **Piggery backing and tailgating:**

The first term is used for gaining entry into a controlled area where access is controlled by or mechanically locked doors either accompanying the authorized worker or immediately following him. An authorized individuals with hands full of computer related objects like tape reels stands near the locked room. When the authorized users arrives and opens the door, the authorized person goes in after along with him. This can be prevented vby mantraps, television cameras monitoring or a stationed guard.

Electronic piggy backing can also take place on a line computer system where individuals use terminals and the identification of the user is verified by the computer system by means of password and signature. Tailgagating involves connecting a computer user to computer in the same session has been interrupted. This situation when a dial-up or direct connect session is abruptly terminated and a communication controller (concentration or packet assembler /dissembler) incorrectly allows a second user to be patched directly into the first user still upon files.

9.6. **Data Diddling: [false data entry]:**

This is done at a time of computer feeding. This is simplest, safest and most common method of committing computer crime .In this method data is changed before or during their input to computer or output from a computer. The changes can be made by anybody associated with or having access to the process of creating, recording, transporting, encoding, examining, checking or converting data entry to a computer. For example forging or counterfeiting documents, exchanging valid computer tapes, floppy discs, pressing extra key of avoiding necessary key.

9.7. Super zapping and scavenging:

This to use whatever is already in the computer. Super zapping is the unauthorized use of utility programmes to modify, destroy copy disclose, insert or use or deny use of stored data in a computer media. In any computer system, which has secure operating mode needs a super programme will by all pass all the modes and controls to disclose the contents in case of emergency. Such utility programmes are required by the system administrator or system programmer but it can become dangerous if it falls in the wrong hand. (The utility programmes are normally used by the systems programmers and computer operators who maintain computer operating system programmers should be secure from unauthorized use).

9.8. Time (or logic) Bomb or trap door: A logic Bomb can erase specified programs or files or cause an application software such as payroll, accounts receivable or the whole system to crash.

10.0. EXAMPLES OF COMPUTER CRIMES:

10.1. Automated Teller Machine Fraud:

ATM Cards are lost or stolen and unauthorized used. The cards under personal identification number (PIN) could be intercepted from mail and unauthorized for withdrawing cash.

10.2. Credit Card Fraud:

Credit cards are stolen and signatures forged. Besides stolen and forged cards, other common credit card related hazards include lost and misplaced cards, fraudulent applications, alteration of cards, counterfeits, collusion between holder and merchants, holder and credit cards company employees, and between holder and credit reporting agencies, fraudulent charges, postal heft, mail order telephone fraud, magnetic strip tampering etc.

10.3. Electronic Funds Transfer Frauds:

The transfer is by cable, telex, through computer networks and various codes are used for transmitting bank codes, receiving bank codes, currency, and data amount in tens, hundreds, thousands, ten thousands, etc, and these codes are added up and used in message. A unscrupulous employee or insider can fraudulently use these codes for illegal transfer of funds.

10.4. Frauds in Electronic Commerce:

The Internet to day is extensively used for banking and commercial services. Many products are advertised on the internet websites. Financial transactions also take

place on the internet. Though these transactions are encrypted authorized persons will have the key to decrypt the message and software also has some authenticated mechanism. But all these can be bypassed or circumvented or fraudulently used by unscrupulous person.

10.5. Fraud manipulating bank accounts:

Several cases of misappropriation of funds manipulation or computer records have been reported. Several banks are cheated through falsification of computerized bank accounts.

10.6. Telecom Frauds:

Telecom Frauds and Computer Frauds are interrelated since computer networks make use of telecommunication lines for wide area connectivity. Local Area Networks are connected with enterprise wide server through dial-up modems, leased line, ISDT (Integrated Service Digital Network) lines VSAT (Very Small Aperture Terminal). Today, telecommunication networks are used for voice data communication, voice mail, E-mail and transmission of fax messages, images and even video conferencing. Electronic mail over the internet is also being used extensively. Cellular or mobile telephoning, pagers and telephone cards are also becoming popular.

Telecommunication fraud is extensively used by organized criminals. These networks facilitate organized crimes such as drug smuggling, money laundering, immigrant smuggling, theft or fraud relating to credit cards, tele marketing frauds and other fraud schemes. All these gangs maintained anonymity for their operations and they extensively use the telecommunication facilities. The losses to telecommunication organizations from fraudulent activities involve millions of dollars.

10.7. Pornography:

An issue that has caused utmost concern is the spread of cyber prone as also sexism, racism, sadomasochism and child abuse or child pornography over the internet. This menace is corrupting the young minds and eroding the basic values of civilized society. Porno sites on the internet are used for producing nude photographs of celebrities and downloading offensive pictures.

10.8. Money Laundering and other organized crimes:

Cases of money laundering and other Hawala transactions over the internet are reported. Research shows that international, majority of people suffer from frauds in many ways as shown in the table below:

Percentage of all referred fraudulent complaints:

Auction Fraud	41.10%
Non Delivery	31.30%
Credit/Debt Card Fraud	11.60%
Investment Fraud	1.50%
Business Fraud	1.30%
Confidence Fraud	1.10%
Identity Theft	1%
Check Fraud	0.50%
Nigerian Letter Fraud	0.40%
Communication Fraud	0.10%

10.9. Computer aided Murder:

In case a suspect committed murder by changing a patient medication information and dosage in a hospital.

10.10. Counterfeiting:

Counterfeiting of Degree Certificates, Registration Certificates of vehicles using DTP systems have been reported.

10.11. Extortion/Blackmail:

Holding out threats of wiping out their computer systems, international gangs of sophisticated cyber terrorists have extorted staggering funds from financial institutions for a number of years.

10.12. Software Piracy:

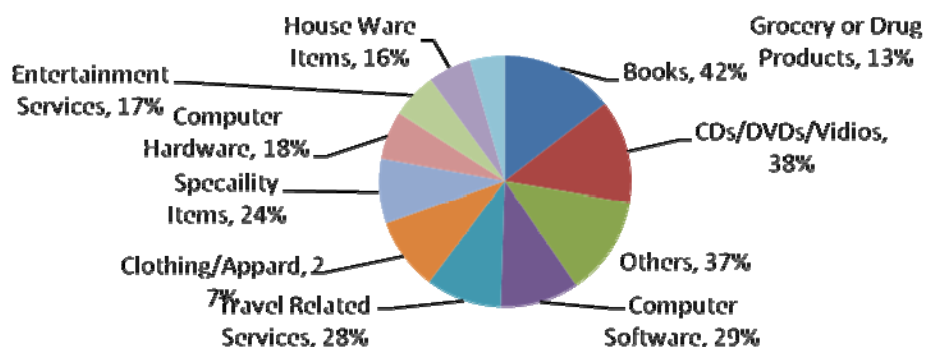
This is the least publicized but yet the most common computer crime. It causes heavy financial losses to Government, Criminal Justice, Academic and industry. Software Piracy is the copying or theft of proprietary software and raw data or information

10.13. Sabotage:

There are several instances of sabotage of computer system through introduction of viruses. Sabotage can be not only in respect of computer or computer systems or computer network; it can be of operating system and programs.

N.B. In summary computer crime is committed in every second and through all avenues of everyday life activities individuals' transverse as shown in the pie chart below:

Computer crime on line (citizen demographics and purchasing Habits)



11.0. CYBER TERRORISM:

It has been recently reported that several; financial institutions in the UK and USA have paid huge sums to international gangs of extortionists and terrorist over the internet. They are called 'cyber' terrorists. Under threat of wiping out computers systems through use of logic bombs, these terrorists have extorted around 400 millions Br pound worldwide from financial institutions. 40 such attacks on financial institutions in London, New York and other European banking centers have been reported since 1993. These institutions have given back mail rather than reporting the matter to the police for fear of lose of confidence by the public in their security systems. This new form of information warfare is a global threat. One of the problems faced by the police is that the crime is carried out of the globally but law enforcement stops at their frontier. The ransom amounts in these cases were paid to off share accounts and the gangs removed these within minutes. Banks, breaking firms and investments houses in the United states, Great Britain and other major financial centers of Europe have secretly paid ransoms to prevent costly computer meltdown and collapse of confidence among their customers, the paper said, in an exclusive report quoting sources in White Hall and Washington. The report investigation had been launched in all the major financial centers around the world, after more than 40 cyber attacks had been unearthed in New York, and other European banking trading to halt by using advanced information warfare techniques learnt from the military. According to American national security Agency [NSA] ,the cyber terrorists have penetrated computer systems using logic bombs [coded devices that can be remotely detonated], electromagnetic pulses and high emission radio frequency guns, which blow a devastating electronic wind through a computer system. The story which was carried as the lead item, said cyber terrorists had also left encrypted threats to the highest security levels, reading now do you believe, we can destroy your computers. The authorities have been un able to stem the attacks, which are though to emanate from US as in most cases banks have failed to notify the police. London police Officials were quoted as saying that investigation had been hampered as senior financiers were hindering inquiries.

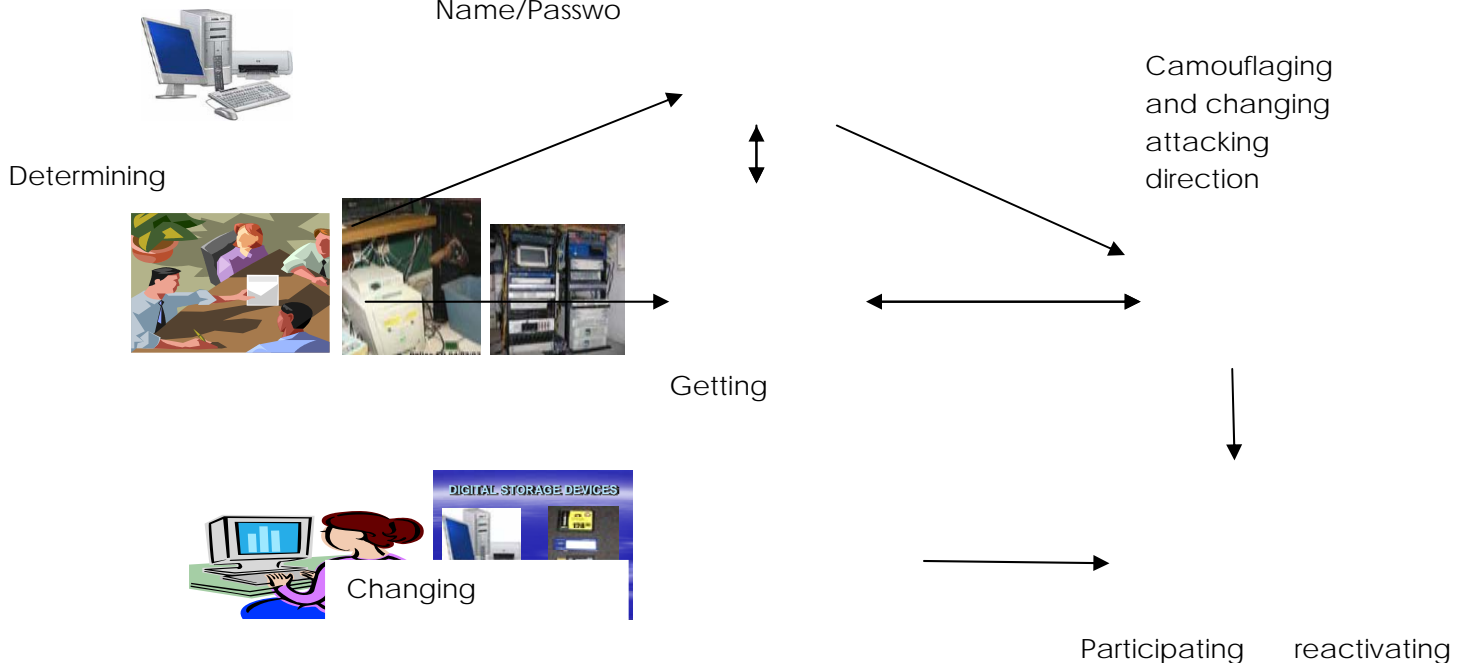
12.0. Means of monitoring violation on internets

- Anti Virus.
- Sniffing (taping).
- Spoofing (camouflaging).
- Pass word break/crack.

12.1. Brief description of attacking sequence (spoofing camouflage) either to new password or to user name

The attack determines his targets and the objectives such as administrator of attacking. In order to attack you should camouflage not to attack directly here they use proxies (which take many addresses and give me another) to find a gap for attacks. You are able to get user data as shown below:

Getting User
Name/Passwo



12.2. How to secure yourself from hackers

- You should know to whom you are communicating through. That is to say do not click any unknown email from your email address, put it in the explorer and access it from the address bar.
- Secure your personal data, do not tell anyone about your password, email or account.
- Secure your personal computer by using personal fire walls, very strong anti virus
- Protect your password use strong, and long pass word. Your password should be more than characteristics, small and capital letters. Use special characteristics like frequently your password.

13.0. Challenges in cyber crime:

- ♣ Cyber cafes connection.
- ♣ Wireless indirect emergency.
- ♣ ADSL technology.
- ♣ Use of proxy (signing without IP Address).

14.0 CONCLUSION:

Thus, computer crimes examined on the backdrop of techniques could be either data-related, software related or simply physical crimes. Physical crimes could be theft of computer equipments or its peripherals, input or output data, physical damage or destruction of computer and peripherals.

At present, there is no specific legislation in our country for defining methodologies of various computer crimes or specifying of quantum of punishment either fine or punishment. The best defense we can have against the computer crimes at present is to educate fellow computer professional, employees and the generation of programmers so that they can make informed choices. This will not solve all computer crimes, but it will reduce the incidents of crime by accident and default. As Police, we do not have to just look on while crime is being committed, the crime should be investigated since expertise is already in place.

15.0. RECOMMENDATIONS:

Cyber Crime is one of the crimes with the largest crime scene, once it occurs it needs through combing and if requires facilitation for the investigation to continue and get competed. Uganda needs to have a facility to report cyber crimes. Thus, it is advisable for the Directorate to put into consideration and open up an office specifically to handle cyber crimes since it is one of the world threats/avenue of crimes. **The There need to set up cyber crime department in Uganda Police with following responsibilities:**

- ⌘ Record complaints and Create a database, which will be examined together with other agencies like Interpol, immigration, forensic bureau, prisons, police and other institutions like banks and so forth that will help in tracking criminals
- ⌘ Given that cyber crime is an international problem, which can be solved through the cooperation with other countries, this can only be achieved through an organized system such as the proposed department/directorate to handle cyber crimes in Uganda.
- ⌘ The department will also create a legitimate database for licensed business authorized to operate in order to crack down culprits of electronic fraud.
- ⌘ Anti fraud squad will be set up in the department to fight the rampant white collar cyber crime that exist in government and private institutions
- ⌘ Train people in Uganda Police in Cyber forensics in order to have adequate manpower for cyber crime investigations.
- ⌘ The following are some of the software's that will be required by the department to fight cyber crime;

1. CDAC's Cyber Forensics Tools for investigation and analysis of cyber crime
 2. TrueBack – Disk Imaging Tool
 3. CyberCheck – Data Recovery and Analysis Tool
 4. EmailTracer – Tool for tracing sender of email
- ⌘ To harmonize the national and international criminal laws that will make Uganda become less cyber crime haven for criminals.
- ⌘ The department will also sensitize the community about cyber crime so as increase community's responsibility to report such case to protect themselves against perpetrators of the crime. The following are issues of concern that the department will caution the public against:
1. Do not check programmes from unknown sources.
 2. Do not accept files with an extension .ext.
 3. Do not log in through phishing pages.
 4. Do not waste time playing games on the internet because the aim is to get money from you.
 5. Do not sign in to Narcotics/Drug.
