By Edris Kisambira

Computer crime, cyber crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. This sort of crime is increasing in Uganda and many people have been defrauded. Edris Kisambira spoke to the deputy director Criminal Investigations Department (CID) Police, Mr. Moses Sakira and below are excerpts.

QN: Cyber crime is known to be thriving in the developed world where there is a lot of e-commerce but we now know that it is also happening in Uganda, what form is it taking from the Police's perspective?

ANS: There is hacking into Internet networks of especially importers of goods from places like Dubai, China and Japan. The unsuspecting business people usually get to discover when either there money has been stolen or the goods they ordered from Europe, China, Japan or Dubai have been diverted to somewhere else. There are also Ugandans who are using the Internet to push through forged travellers' cheques, which they use to purchase goods from unsuspecting business people in Europe, Dubai, China and Japan. What has happened is that manufacturers or traders outside Uganda dispatch goods based on the forged travellers' cheques as confirmation

for payment only to discover they cannot cash the cheques – now these are Ugandans defrauding foreign business people.

Ugandans are also in the habit of forging ministry tender documents claiming they have secured large contracts; and when these unsuspecting foreigners send the goods to Uganda, the culprits receive the goods and cut all communication links. Cases have also been reported where money is way-laid by cyber criminals who hack into people's email accounts; they impersonate the real owners of such email addresses, convince the senders of the money that they have changed bank accounts and in the process, such money gets diverted. People are also defrauded on cell phones but the problem with that is people are reluctant to report to Police.

QN: Is it a one-way or there are also consumers here in Uganda being defrauded?

ANS: There are many foreign websites based in places like Japan that defraud unsuspecting Ugandans especially those that are importing cars. Rogue Japanese car dealers are defrauding Ugandans online and we have received many complaints. People pay money to Japanese fraudsters and money is lost through online transactions. A case just came to our attention after someone lost US$8,000 as he attempted to purchase two cars from Japan.

QN: To what scale is it happening here? I mean how many of such cases do you receive maybe in a month?

ANS: I don't think they are too common but like I said there could be many more such cases that do not get reported to Police. But I also think that the cases that people get to report are those involving big sums of money or when the value of stolen goods is high.

QN: What measures or mechanisms have the Uganda Police put in place to handle cyber crime considering that the police human resource has no skills and with technology limitations?

ANS: To start with, the Police structure now has a full directorate of Information Technology (IT) here at the Police headquarters. We are also developing an IT laboratory with the help of development partners, that will enable us investigate these crimes when they occur but also catch-up in terms of technology and the training of Police personnel. We realize that our human resource capacity in the IT area is still low, but we are carrying out training whenever we get the opportunity.

We have in the past benefited from assistance from Egypt and from the US through the United States Department for International Development (USAID). As members of International Police, we have received some basic IT training but I think it needs to be taken to a higher level. The challenge though is that IT evolves very fast all the time and training should be continuous but the other challenge is it is expensive to train people in that area.

QN: As we speak, the Penal Code does not provide for cyber crime and the few people that have been prosecuted have not received deterrent sentences, what does that mean?

ANS: There are aspects of cyber crime where the law does not help us and we need reforms in those instances. Examples are messages like emails and short message services (SMS) – these things are not admissible in court yet a lot of times those are the exhibits you need to win a case. We find the need for such information to be admissible. But even though 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. These categories of crimes are provided for in the Penal Code and can be prosecuted even if they were of a cyber nature.

QN: A lot of Ugandans (especially those in the import trade) do not yet know that there are ‘new generation’ thieves who are getting more sophisticated every day, is the Police in any way thinking of making them aware?

ANS: As the Police, we study crime trends and we are always sensitising the general public of the modes of operation of criminals and cyber crime is no different.

QN: Laws that will punish cyber criminals are coming but even when they are operational, what are the challenges you still foresee?

ANS: Finding those Ugandans within and outside the Police who are skilled in IT and remunerating them well will be a big challenge. IT is new and employing the right personnel who are skilled in this area is something the Police will grapple with. The other challenge of course is the resources the Police need to follow- up these cases. Some of these cases require for instance Uganda Police officers to travel to the countries where the crimes have been committed instead of relying on messages and telephone calls to Japan that do not help much. And the right to access the databases of the companies that provide telephone and Internet services is a challenge.

QN: How do you define computer or cyber crime?

ANS: Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal 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) and electronic fraud.