CYBERCRIME BAROMETER, A UGANDA POLICE CENTENARY PLUS AWARENESS CAMPAIGN PAPER

OVERVIEW

"In order to secure life and property in a committed and Professional manner, in partnership with the public, so as to promote development and have an Enlightened, Motivated, Community Oriented, Accountable and Modern Police Force geared towards a Crime free society it is only but prudent that we engaged in such online platforms to create awareness about the existing cyber threats in Uganda and the entire world at large."

Digital technologies and the internet have transformed our everyday lives since we can n access information, conduct business, keep in touch with family and friends, and engage with Government (www.askyourgov.ug/)

However with such advancement in technologies there has emerged the new wave of crime termed as ***cybercrime***.

Cyber-crime sometimes called e-crime is the type of crime committed through communication technology. The crimes are committed using computer systems and the computer networks are used to facilitate the omission/commission of the offence. These are committed through Internet such as cyber harassment, anti-social activity, money laundering, threatening behavior, narcotics, human trafficking, terrorism, Denial of Service Attacks, to mention but a few.

Literally, a computer system includes the computer along with any software and peripheral devices that are necessary to make the computer function. These are laptops, desktops, iPhones, some smartphones, tablets, servers and others. These systems now make the Internet (i.e. global network of computers).

Cybercrimeis no longer about those who seek to break into computer systems for fun but to cause further breaches upon access. The criminals behind such crimes are organized, and seek to take advantage of those using internet services. Whether this is for financial gain, or as threats to children, the effect on the victims can be devastating. The most vulnerable members of our society are all too often the victims – from young people threatened by bullying or sexual predators to the elderly who provide easy prey for organized fraudsters.

Cybercrimes, as well as financial crimes are serious emerging challenges that threaten the security and stability of our country, and our region and beyond. To fight these transnational and cross border crimes requires regional, and, even, African-wide cooperation and collaboration, as well as Interpol support.

To underscore this, during the year under review, Eastern African Police Chiefs Cooperation Organization (EAPCCO) and Southern African Regional Police Chiefs Cooperation Organization (SARPCCO) carried out a simultaneous operation code named '*Usalama*' in a bid to combat these crimes. It was conducted from 16th – 18th July 2013 targeting Drug trafficking, Human Trafficking/Migrant Smuggling, Motor vehicle thefts and illicit proliferation of small arms and light weapons. It was the first operation of its kind and it registered an improbable success.

CYBERCRIME STATISTICS

In reference to the research done by the Collaboration on International ICT policy in East and Southern Africa (CIPESA 2014), the increased Internet penetration and Tele-density in the East African region, Uganda in particular being at 20% and 52% respectively, the access to the social network sites such as Facebook, YouTube and twitter has been made easy and thus the population can now actively influence service delivery, policies and even management of public goods.

As per the Uganda Police Annual Crime and Road Safety Report of 2012 a total of 62 cases were reported and investigated in which about 1.5 billion UGX (579,000 USD) were lost through hacking victims mails among other means.

Furthermore between the month of August and November 2014 only, mobile money frauds caused a loss of over 207 million UGX (80,000 USD) to the users. Within the same year, ATM/VISA frauds led to a loss of over 1.2 billion UGX (460,000 USD) from over 700 victims by use of scheming devices installed onto ATMs located in Kampala and other areas.

Cyber-crimes reported in 2013 were 45 cases compared to 62 cases in 2012. However these resulted into a loss of about 18.1 billion UGX (7 Million USD). This implies that more grave losses were made subsequently despite the reduction in reported cases.The crimes included Electronic frauds, Phishing (password harvesting), Email hacking, pornography/defamation, offensive communication,mobile money frauds, SIM Card swapping and ATM/VISA frauds among others.

WHAT ARE THE MAIN CYBERCRIME TOOLS?

Criminals have the capability of making or developing their own tools in addition to the legitimate or publicly available software like peer to peer used in sharing files and illegal images. Business men and women might believe their most valuable assets are those they can see and put their hands on. For example real estate, stores, merchandise and people.

But today’s most dangerous thieves are looking for less tangible but no less precious loot that is to say corporate and customer data which is the most transactions used in paying tangible assets.

Hacking has evolved from the activity of a small number of technical individuals to an increasingly mature marketplace where technical skills and data can be purchased by criminal groups to carry out specific attacks.

Staging Your Attack, it includes generally five stages to a targeted attack that is to say Research, intrude using reached information, propagate the malware to machines on a network, infect the data on machines by installing additional tools, and exfiltration of the gathered data.

Scaling Attacks: The vulnerability can be installed as Point Of Sale of one small grocery store in one bank – but it’s likely that the same vulnerability and system configuration will work in airport machines at other franchises of the same brand, opening up wider avenues for data stealing.

Social Engineering: Often, employees help out cybercriminals without knowing they're doing so via social engineering ploys. Like if in need of information about the organizational chart, the location of a data center or the technology in use, they call someone who would know, pretend to be from another department and ask. They have official-sounding emergencies requiring the needed information help pry the information loose, as does knowing the name of boss.

Phishing: Criminals use social media to discover lots of valuable information by setting up a dummy Facebook account which is use to made friendly requests. The victim will then reveal where he/she went to high school or college, their mother's maiden name, their birthday and facts about their job. All of these are valuable hints at passwords, system challenge questions and information to grease the skids of a targeted campaign.

Reinvent Old Web and E-Mail Attacks: Advanced attackers use strategic Web compromises to infect targets via drive-by-download. Old Web filtering technology won't always work; techniques such as initiating IP address-specific malware downloads can get around defenses that depend on reputation filtering.

Salami techniques: Quiet and slow exfiltration makes it easier for criminals to steal large stores of information without setting off alarms that shut down at midstream. Most companies don't set up firewalls to block outbound traffic, which gives several options. Public Web traffic can be efficient for slowly leaking data off the network.

WHO ARE THE PERPETRATORS OF ONLINE CRIME?

There are criminals mainly for personal financial gain or funding terrorist attacks. These mainly target government, business and public. They sometimes use virtual networks in a web forum not meeting in person. These networks have a thousand plus members but run by a small number of specialized online criminals. These criminals divide their roles as hacking, spamming, compromising machines and others. The organized crime groups are sometimes sophisticated in that they operate within a cellular structure and are well collaborative because competition is not always on their agenda.

Other criminals are not for financial gain e.g. threats to children, hates, harassment, political extremism etc. like targeting children for sexual abuse through social networks, chatting, messaging; creation of images and share them online ; luring vulnerable group into some form of exploitation; racial or religious hatred, e.tc

WHAT ARE THE THREATS TO THE PUBLIC AND BUSINESS ?

PUBLIC

1. Online fraud ranging from credit and debit card fraud, lottery scams, non-delivery fraud, online auction, health scheme issuance, salami technique frauds, e-tax payments and others.
2. Identity theft to compromise private information like financial information for personal gain or for sale like human trafficking. Bank account holders may be tricked to reveal private data through fake emails and websites or their account holding computers can be infected with a malware that automatically intercepts and forwards data to the criminal.

3. On line Child exploitation by the use of Internet through gaming, social networking, research tools etc. Children use Internet and meet people parents call strangers. It is through Internet that child sex abuse within families is recorded and shared through images.
4. Hate crimes and terrorism.

BUSINESS

Dependency on Internet and electronic communication by the commercial sector in business transactions is on a high rise in developing countries. There are a number of ways the businesses are affected:

1. Like public, business environment has fraud concerns through goods being paid for with stolen or forged credit cards.
2. Data insecurity. Breaching of data for commercial is very risky for companies. These can be caused externally or internally.
3. Intellectual property theft. Illegal file sharing using peer-to-peer technology over the Internet affects the creativity of the industry sector.

ONLINE SAFETY TIPS

- Set strong passwords, and don't share them with anyone.
- Keep your computer updated with the latest anti-virus and anti-spy ware software, and use a good firewall.
- Never send your online account details through an email and think carefully before you give away any personal or financial information.
- Limit the amount of personal information you post online, and use privacy settings to avoid sharing information widely.
- Never enter your personal information on a website if you are not certain it is genuine.
- Don't click on the link provided in an email or call the phone number provided; instead, find the business's contact details through a general internet search.
- Check the privacy settings and think about who you really want to have access to your personal information.
- Be careful about what personal information you put on the internet, because scammers can use these details to guess your passwords or to commit fraud.
- Check how much information is available about you on the internet by typing your name into a search engine and see how many hits you get.
- Don't be lulled into a false sense of security—online 'friends' may not be who they say they are.
- If you receive an unexpected request for money from what appears to be a friend, try to contact that friend or their family or friends to verify the request. Do not use any of the contact details in the message.

DEDUCTION

We are duty bound and have the conviction to do more to improve public awareness oncybercrime through our online platform to deal with things like;

- What it looks like,

- who is doing it and
- What the public and business can do to protect themselves from cyber criminals.

These and other measures will allow us to take action against cyber criminals from the organized groups at the top end right through to the long tail of organized criminality that exists underneath. Cybercrime threatens our safety, undermines our economy, and the scope and sophistication of cybercrime in the 21st Century demands an equally sophisticated and ambitious strategy to tackle it.

Compiled by:

Haguma Jimmy
Acting Commissioner of Police – Electronic and Counter Measures Department
Directorate of ICT – Uganda Police Force
Jimmy.haguma@upf.go.ug or hagumaj@gmail.com
@hagsecm