INFORMATION AND CYBER SECURITY:

EMERGING TRENDS IN SOCIAL MEDIA COMMUNICATION.

BY

PROF. HENRY EMBEYWA.

MACHAKOS UNIVERSITY.

INFORMATION TRENDS AND CYBER SECURITY

- IN TODAYS WORLD, INFORMATION IS INCREASINGLY DIGITAL, MAKING IT EASY TO MISUSE.
- USING INTERNET TO SHARE OR COLLABORATE CREATES ROOM FOR INVATION.
- ORGANIZATIONS ARE STRUGGLING TO PROTECT THEIR CONFIDENTIAL INFORMATION AND TO KEEP PACE WITH THE INCRESINGLY STRINGENT LAWS THAT PROTECT CONSUMER AND EMPLOYEE PRIVACY, AND INFORMATION SECURITY COMPLIANCE IS THEREFORE BECOMING MORE DIFFICULT.
- SECURITY BREACH MAY CAUSE CUSTOMERS AND REGULATORS TO LOSE TRUST IN RELIABILITY, REPUTATION MAY SUFFER, AND FINANCIAL LOSES MAY BE INCURRED.

CYBER SECURITY

- CYBER SECURITY (IT SECURITY) IS THE PROTECTION OF COMPUTER SYSTEMS FROM THE THEFT AND DAMAGE TO THEIR HARDWARE, SOFTWARE OR INFORMATION, AS WELL AS FROM DISRUPTION OR MISDIRECTION OF THE SERVICES THEY PROVIDE.
- FACTS:
  - EVERY COMPUTER IS HACKED
    - WHEN AN APPLICATION YOU DONOT WANT KEEPS APPLYING NO MATTER WHAT YOU DO.
  - MOST COMPANIES OR ORGANIZATIONS DON'T KNOW THE WAY THEY ARE SUCCESSFULLY ATTACKED THE MOST.
    - STUDY THE LOGS AND ASK EXPERTS
  - A CRITICAL GULF EXISTS BETWEEN REAL AND PERCEIVED THREATS.
    - VULNERABILITY SCANS, SIZE OF DAMAGE AND HIGHEST PROBABILITY
  - FIREWALLS AND ANTIVIRUS SOFTWARE ARE NOT THAT IMPORTANT.
    - FIREWALLS PREVENT AN UNAUTHORIZED CONNECTION ATTEMPT TO AN EXISTING VULNERABLE SERVICE. MOST OF THE THREATS ARE CLIENT-SIDE THREATS, INITIATED BY THE END USER. NEW VIRUSES CAN ESCAPE AN ANTIVIRUS PRODUCT.
  - TWO PROBLEMS ARE ALMOST 100 PERCENT OF THE RISK.
    - UNPATCHED SOFTWARE OR A SOCIAL ENGINEERING EVENT WHERE SOMEONE IS TRICKED INTO INSTALLING SOMETHING THEY SHOULD NOT.

COMMON THREATS

- DATA THEFT.
- ATTACKS FROM WEB APPLICATIONS.
- DISTRIBUTED SERVICE DENIAL.
- RANSOMWARE LOCK OUT OR BLACKMAIL.
- STOLEN BIODATA DUE TO SHARED PASSWORD OR FORGOTEN PASSWORD.
- FLASH LETING.
- MALWARE.
- INSIDER THREATS FROM EMPLOYEES.
- PHISHING.(THE HTTP-TRICK).
- LACK OF SECURITY SKILLS.

MEANING OF CYBER CRIME

- **Cyber crime**, or **computer related crime**, is crime that involves a computer and a network.
- The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)“
- Cybercrime may threaten a person or a nation's security and financial health.
- Issues surrounding these types of crimes have become high-profile, particularly those surrounding:
  - hacking, copyright infringement, unwarranted mass-surveillance, child pornography, and child grooming.
  - There are also problems of privacywhen confidential information is intercepted or disclosed, lawfully or otherwise.
  - From the perspective of gender, 'cybercrime against women' include "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones“.

WHO IS INVOLVED IN CYBER CRIME?

- Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes.
- Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare.
- Employees, their accomplices.
- Hackers and Bloggers.
- Service providers.
- Creative ICT Experts.
- Criminals.

FRAUD AND FINANCIAL CRIMES

- Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:
  - Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;
  - Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
  - Altering or deleting stored data;
  - Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information.

PHISHING AND SOCIAL ENGINEERING

- A variety of internet scams, many based on phishing and social engineering, target consumers and businesses.

- **Cyberterrorism**
  - Government officials and information technology security specialists have documented a significant increase in Internet problems and server scans since early 2001,such intrusions being part of an organized effort by cyberterrorists, foreign intelligence services, or other groups to map potential security holes in critical systems.
  - A cyberterrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.
  - Cyberterrorism in general can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda piece in the Internet that there will be bomb attacks during the holidays can be considered cyberterrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

PHISHING AND SOCIAL ENGINEERING……..

- **Cyber extortion**

  - **Cyber extortion** occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybere xtortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.

PHISHING AND SOCIAL ENGINEERING…..

- **Cyberwarfare**
  - The U.S. Department of Defense (DoD) notes that the cyberspace has emerged as a national-level concern through several recent events of geo-strategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.
- **Computer as a target**
  - These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet:
- Crimes that primarily target computer networks or devices include:
  - Computer viruses
  - Denial-of-service attacks
  - Malware (malicious code)

INTERNET FRAUD, SPAMMING, PHISHING, AND CARDING (FRAUD)

- **Computer as a tool**
  - When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult.

  Crimes that use computer networks or devices to advance other ends include:

  - Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime)
  - Information warfare: battle space use and management of information technology in pursuit of a competitive advantage over an opponent. (misinformation, propaganda, and deception, jamming, fooling and monitoring each others efforts).
  - Phishing scams: attempting to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
  - Spam: flooding the internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. E.g. commercial advertising, often of dubious products, get-rich quick schemes, or quasi-legal services.
  - Propagation of illegal obscene or offensive content, including harassment and threats
  - The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.
  - Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware.[Or, they may contain links to fake online banking or other websites used to steal private account information.

OBSCENE OR OFFENSIVE CONTENT

- The content of websites and other electronic communications may be distasteful, obsceneor offensive for a variety of reasons. In some instances these communications may be legal.
- The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.
- One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.
- **Harassment**
  - Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties. Harassment on the internet also includes revenge porn.

DOCUMENTED CASES

- One of the highest profiled banking computer crime occurred during a course of three years beginning in 1970. The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over $1.5 million from hundreds of accounts.
- A hacking group called MOD (Masters of Deception), allegedly stole passwords and technical data from Pacific Bell, Nynex, and other telephone companies as well as several big credit agencies and two major universities. The damage caused was extensive, one company, Southwestern Bellsuffered losses of $370,000 alone.
- In 1983, a nineteen-year-old UCLA student used his PC to break into a Defense Department international communications system.
- Between 1995 and 1998 the Newscorpsatellite pay to view encrypted SKY-TVservice was hacked several times during an ongoing technological arms race between a pan-European hacking group and Newscorp. The original motivation of the hackers was to watch Star Trek re-runs in Germany; which was something which Newscorp did not have the copyright to allow.
- On 26 March 1999, the Melissa worminfected a document on a victim's computer, then automatically sent that document and a copy of the virus spread via e-mail to other people.
- In February 2000, an individual going by the alias of MafiaBoy began a series denial-of-service attacks against high-profile websites, including Yahoo!, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN. About fifty computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in DDoS attacks. On 3 August 2000, Canadian federal prosecutors charged MafiaBoy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks.
- The Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legitimate. But apparently the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. The RBN has been described by VeriSign as "the baddest of the bad". It offers web hosting services and internet access to all kinds of criminal and objectionable activities, with an individual activities earning up to $150 million in one year. It specialized in and in some cases monopolized personal identity theft for resale. It is the originator of MPackand an alleged operator of the now defunct Storm botnet.

DOCUMENTED CASES

- On 2 March 2010, Spanish investigators arrested 3[*clarification needed*] in infection of over 13 million computers around the world. The "botnet" of infected computers included PCs inside more than half of the Fortune 1000 companies and more than 40 major banks, according to investigators.
- In August 2010 the international investigation Operation Delego, operating under the aegis of the Department of Homeland Security, shut down the international pedophile ring Dreamboard. The website had approximately 600 members, and may have distributed up to 123 terabytes of child pornography (roughly equivalent to 16,000 DVDs). To date this is the single largest U.S. prosecution of an international child pornography ring; 52 arrests were made worldwide.[26]
- In January 2012 Zappos.com experienced a security breach after as many as 24 million customers' credit card numbers, personal information, billing and shipping addresses had been compromised.[27]
- In June 2012 LinkedIn and eHarmony were attacked, compromising 65 million password hashes. 30,000 passwords were cracked and 1.5 million EHarmony passwords were posted online.[28]

DOCUMENTED CASES

- December 2012 Wells Fargo website experienced a denial of service attack. Potentially compromising 70 million customers and 8.5 million active viewers. Other banks thought to be compromised: Bank of America, J. P. Morgan U.S. Bank, and PNC Financial Services.
- April 23, 2013 saw the Associated Press' Twitter account's hacked - the hacker posted a hoax tweet about fictitious attacks in the White House that they claimed left President Obama injured.This hoax tweet resulted in a brief plunge of 130 points from the Dow Jones Industrial Average, removal of $136 billion from S&P 500 index,and the temporary suspension of AP's Twitter account. The Dow Jones later restored its session gains.
- In May 2017, 74 countries logged a ransomware cybercrime, called "WannaCry".

DEALING WITH CYBER CRIME

- LEGISLATION- STRONG LAWS WITH HIGHER PENALTIES.
- INFORMATION SECURITY AND CYBER RISK AWARENESS.
- CYBER CRIME INVESTIGATION DEPARTMENT/UNIT.
- COLLABORATION AMONG SERVICE PROVIDERS.
- COMPUTER CRIME DETECTION AND PROSECUTION.
- **Investigation**
  - A computer can be a source of evidence as it may contain records of value to criminal investigators in the form of a logfile. In most countries, Internet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide Data Retention Directive (applicable to all EU member states) states that all E-mail traffic should be retained for a minimum of 12 months.

DEALING WITH CYBER CRIME……

- THE USE OF INFORMATION SECURITY EXPERTS (HACKERS INCLUDED).
- CREATING AWARENESS AMONG INTERNET USERS ON INFORMATION PROTECTION AND TACTICS USED BY CRIMINALS.

- READ:
  - BBC-NEWS ON CYBER SECURITY
  - THE HACKER NEWS
  - TECHNEWSWORLD
  - THREATSPORT

THANKYOU AND GOD BLESS YOU ALL.