Digital Security Webinar

Unmasking Digital Terrorism | The effect on Civil Society in Uganda

Digital Terrorism (our definition)

The unlawful use of ~~violence~~ the internet and or digital media to cause damage, intimidation, fear and loss, especially against ~~civilians~~ civil society.

- Digital Terrorism usually manifests in several forms;
  - Fraud
  - Spying
  - Assault
  - Theft
  - Censorship

Digital Fraud

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Ransomware is a type of malicious software that carries out a crypto viral extortion attack that blocks access to your data until a ransom is paid and displays a message requesting payment to unlock it.

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access

Digital Spying

Surveillance is the monitoring of computer activity and data stored on a hard drive, or data being transferred over computer networks such as the **Internet**. The monitoring is often carried out covertly and may be completed by governments, corporations, criminal organizations, or individuals.

Hacking is unauthorized intrusion into a computer or a network. Usually by modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective.

Phone Tapping is the monitoring of telephone and Internet conversations by a third party, often by covert means. .

Digital Assault

Denial of Service Attacks This is where the perpetrator seeks to make a computer or a network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet or network

Vandalism in this case, the perpetrators either use malicious software to cause damage of loss or data rather than stealing or misusing the information for their gain.

Bullying/Harassment repeated behavior and an intent to harm and can include posting rumors about a person, threats, sexual remarks, disclose victims' personal information, or pejorative labels (hate speech)

Digital Theft

Software Piracy This theft of software through illegally coping of genuine programs and software or the use of counterfeit products intended to pass for the original

Identity Theft the perpetrators, obtain access to a victims digital identity, i.e. phone number, email address and use to either for their personal gain or to cause damage or loss to the victims reputation or financially

Physical Burglary in this case, the perpetrators break into the victims offices or premises and steal computer hardware or data.

Digital Censorship

Internet Blockades This is the suppression or denial of access to resources or information published or viewed on the Internet

Legislative Climate in this case, the perpetrator (governments) use the legal framework such as laws, law enforcement to suppress access and the right to freedom of speech.

Internet Access Intermittent connectivity or the lack of access in terms of bandwidth, the cost of Internet connectivity, frequent power outages and blackouts, a lack of effective maintenance and scheduled patching, access to skilled human resources, etc. These limit the capability of civil society.

Challenges

Although emphasis is on Internet security, it is essential to understand that Internet security, computer network security and traditional information security practices are all related, whose problems and solutions also highly overlap.

The main challenges to digital security for civil society can be summed up among;

- A shortage of skilled human resources
- Limited resources to allocate for digital security
- Limited levels of awareness/capacity for digital security
- A general lack of awareness of the risks involved in the use of ICT
- Weak ICT governance among individual organizations

Vulnerabilities

It is evident that more than 90% of civils society use software that is out-of-date and/or unpatched, and therefore make civil society especially vulnerable to attack.

- Software which is no longer supported by its developers, and for which security upgrades are no longer available
- Devices being sold with either pirated, out-of-date or unpatched software.
- An inability or unwillingness to upgrade or patch the applications or maintenance on a regular basis
- Inadequate physical security practices
- Lack of transparency and reports structures regarding digital attacks, limit knowledge f the magnitude of digital incidents.

.

Digital Security Principles

- **Awareness:** An understanding of security risks, along with how they can impact us and develop a preparedness to recognize the risk and manage it
- **Responsibility:** Taking responsibility for the management of digital security risks. Due to the fundamental nature of the Internet, one should take into account the potential impacts of one's actions, or inactions, on other stakeholders before taking action.
- **Cooperation:** Engage in ongoing digital security dialogues to effectively counter new and persisting threats. Digital security cannot be achieved alone. There is a need for cooperation and collective responsibility among all stakeholders,

Mitigation Measures

Civils society should develop a multi-stakeholder model and a collaborative security approach;

- Develop an nation wide digital security collaboration, coordination and response committee; Digital Security Alliance
- Engage in capacity building and knowledge sharing by facilitating Information exchange through a national multi-stakeholder structure.
- Support existing regional support structures to coordinate security incident response and pre-response (SFPs)