March
6, 2023

Technical Assistance for Developing Countries

Priorities for Improving Capacity of Public Sector and Civil Society Organizations

Mariya Heletiy
ISAR Ednannia

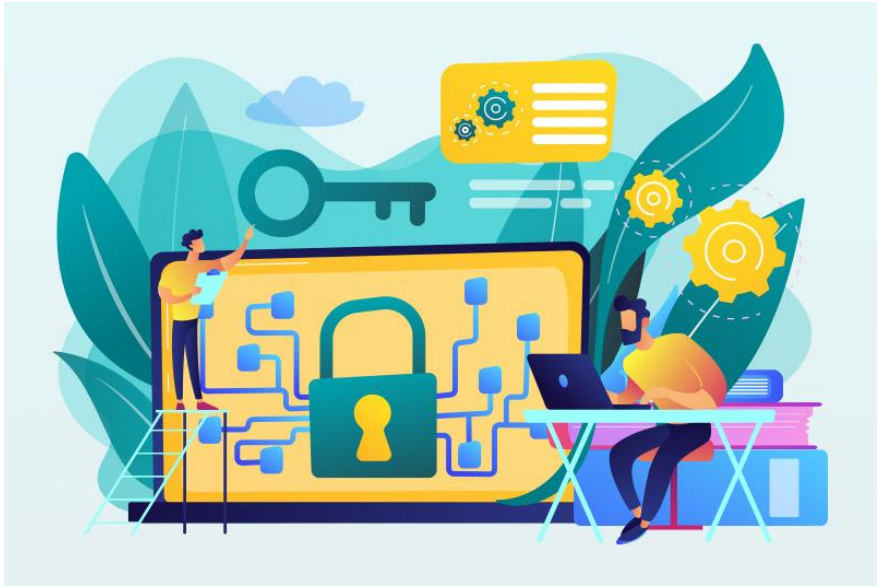
Cyber Challenges in Developing Countries

New technologies, smart devices, internet have benefits and risks:

- May target individuals, business groups, governments and bring harm to a computer or a group of computers in one network
- Can be used for illegal activities to bring harm to users, CSOs and public sector
- May affect CSO operation (financial losses, breaches of sensitive data, failure of systems) and reputation

Cyber Challenges in Developing Countries

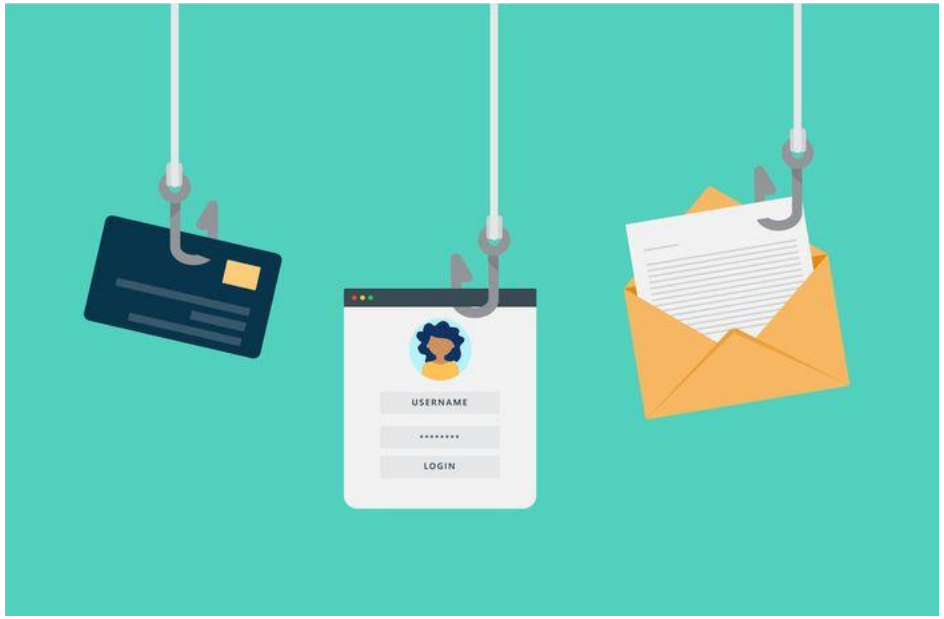
- May lead to hacking of websites, illegal online content or scammers
- Lack of regulations in area cybersecurity and consistency in cyber security regulation in different countries
- Lack of sufficient security measures to protect these technologies



- Security vulnerabilities/security holes in systems (weak authentication methods and passwords; lack of strict security models and policies) may allow a foothold inside the targeted environment

Cyber Threats in Developing Countries

- **Using computers or devises** for crimes
- **Individual Cyber Crimes** targeting individuals (phishing scam, cyberstalking)
- **Cyber Crimes** targeting CSOs incl. malware attacks and denial of service (DDOS) attacks
- **Property Cybercrimes** target intellectual property rights or financial information
- **Society Cybercrimes** the most dangerous form that includes cyber-terrorism



Cyber Threats for Civil Society in Developing Countries

- **Phishing Scam** (targeting and tracking user by sending fake messages to get sensitive information about the user)
- **Identity Theft** - cybercriminal uses another person's personal data (credit card numbers or personal pictures) without their permission to commit a fraud or a crime
- **Ransomware Attack** (malware to encrypt company data for a ransom in order to renew access to the encrypted data)
- **Hacking/Misusing Computer Networks** (unauthorized access to computers or networks)
- **Internet Fraud** (banking frauds, etc.)

Cyber Threats for Civil Society in Developing Countries

- **Cyber Bullying** or internet bullying (incl. sending or sharing harmful and humiliating content about someone else which causes embarrassment)
- **Cyber Stalking** unwanted persistent content from someone targeting other individuals online with the aim of controlling and intimidating (e.g. unwanted continued calls and messages)
- **Social Media Frauds** use of social media fake accounts to perform any kind of harmful activities (e.g. impersonating other users, organizations or sending intimidating or threatening messages)
- **Intellectual-property Infringements** violation or breach of any protected intellectual-property rights (e.g. copyrights and industrial design)

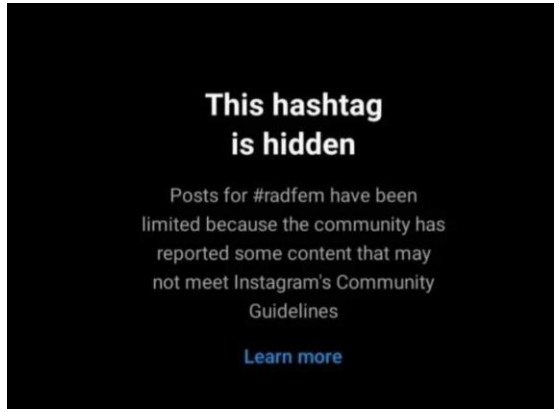
Cyber Crimes Examples

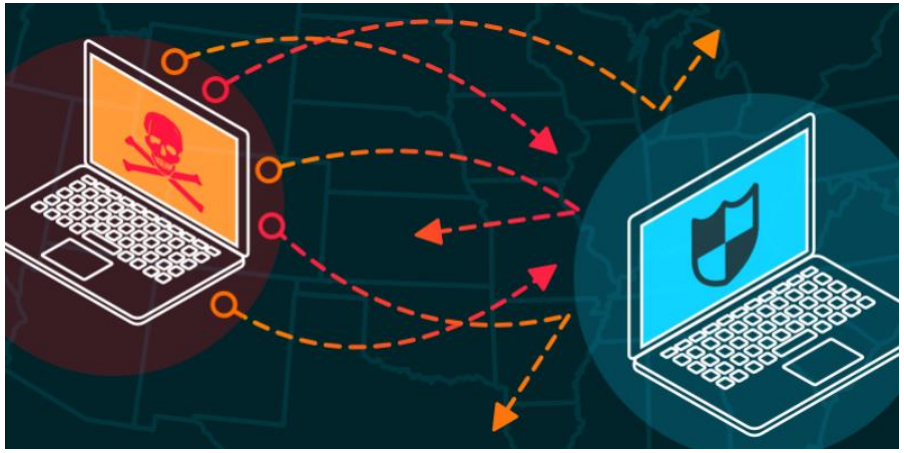
Targeted phishing attacks with harmful software and attacks on media websites

Example: Whisper Gate malware coded access to data on Windows OS in systems of public and private entities + CSOs. Affected organisations received a request with the topic "Court Request No. from Sloviansks City Court" Emails were sent from the domen ***court[.]gov[.]ua.*** *In the letter they were requested to provide financial information with the request to complete doc in pdf format to have possibility to manage the device.*

Cyber Crimes Examples

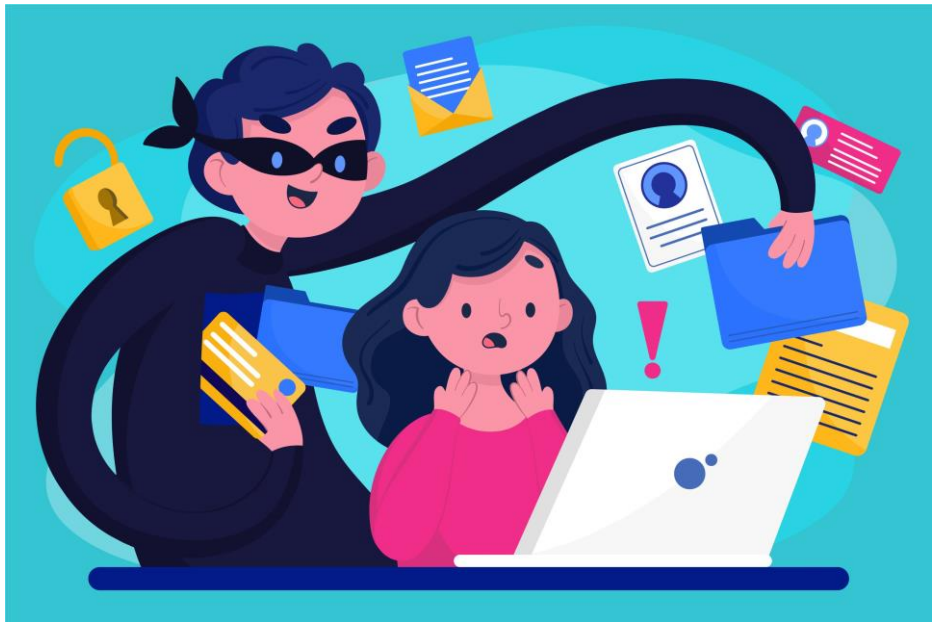
- **DDoS and other attacks on public and media websites.** Attacks on websites of Institute of Mass Information or public institutions
- **Blocking of sensitive content for social media** (because of violence, killings, picture of dead people etc.) sometimes without any reasons
- **Cloning of webpages of charity in social media to collect funds** (e.g. fake accounts of Charities “Come Back Alive” and “Children Voices” in social media positioned as reserve profiles)





Cyber Crimes Examples

- **Surveillance** by criminals, authoritarian regimes, during wars (checking smartphones, social media, emails)
- **Propaganda** through social media (Facebook, Instagram) – empty pages “Only Truth”, “Strength in Truth”



Recommendations

- Adopt **Convention** to combat misuse of technologies for criminal purposes at the international level
- Support development of **guidelines for social media owners** to ensure moderation of content in countries under wars/conflicts/disasters etc. (e.g. inability to delete sensitive content)
- Develop **guidelines to Standards of Community** with exceptions from rules regarding violence, demonstration of nude body etc.
- Support **development of state legislation** to regulate use of technologies

Recommendations

Strengthen capacity of CSOs and public authorities in cyber security + Provide funding for:

- Equipment and up-to-date security software (antivirus and firewalls) or discounts
- Implementing the best security settings
- Trainings for public authorities and CSOs in cyber security
- Building regional partnerships for counteracting cyber crimes

Mariya Heletiy
Deputy Chief of Party
USAID Ukraine Civil Society Sectoral Support Activity
ISAR Ednannia

m.heletiy@ednania.ua

ISAR Ednannia
Data from Cyber Security Lab & Institute of Mass Information