Issue 001

Why Civil Society Organisations in Uganda Needs to Worry

DIGITAL INSECURITY | A THREAT TO CIVIL SOCIETY

DIGITAL SECURITY ALLIANCE

Digital Insecurity

by Defenders Protection Initiative

Civil Society Organisations in Uganda are regular victims of fraud, system breaches, phishing, ransomware, account hijacks, etc. in an increasingly insecure digital world.

They are however, ill-equipped to face these attacks; they have inadequate financial resources to hire skilled and talented IT professionals and services, to procure valid software licenses, IT equipment and IT infrastructure to secure their systems and information.

What is Digital Security?

To keep our personal information private means protecting our digital Identity, digital Assets and Technology

Digital identity is the network or Internet equivalent of your physical identity. Digital asset is any content owned by an individual/entity(organisation) that is stored in digital form while Digital technology is any hardware/software that generates, stores and processes data/content. Digital security includes the tools and practices used to secure your identity, assets and technology.

The Digital Security Conference 2017

The Inaugural digital security conference 2017 is an initiative by DPI that is targeting the leadership of Civil Society Organizations (CSOs) including Executive Directors, CEOs, Program Managers, etc. to provide them with insight into the different digital security vulnerabilities that might put their organisations and information at risk.

Why Civil Society Organisations Should Worry

CSOs in Uganda are increasingly adopting Information and Communication Technology and the Internet to do their work. However, there are some motivated actors that have developed the capacity to manipulate, monitor, subvert and destroy electronic information.

Institutionalized surveillance and censorship is growing and the lack of security for digitally stored or communicated information is becoming a major problem for human rights defenders. On the other hand, this digital age has ushered in some previously unknown problems and vulnerabilities

Digital Security Alliance

The DSA is a coalition of organisations and individual digital security experts working towards securing the digital assets of civil society, human rights defenders, journalists and other activists in the face of threats posed by powerful corporations, unscrupulous criminals, state and other non-state actors.

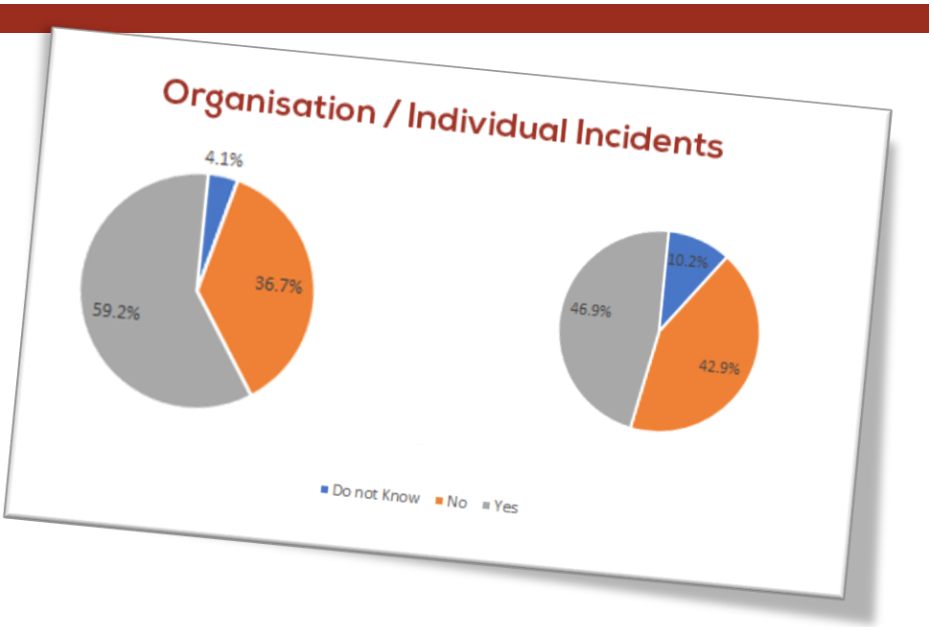
Empowering Civil Society

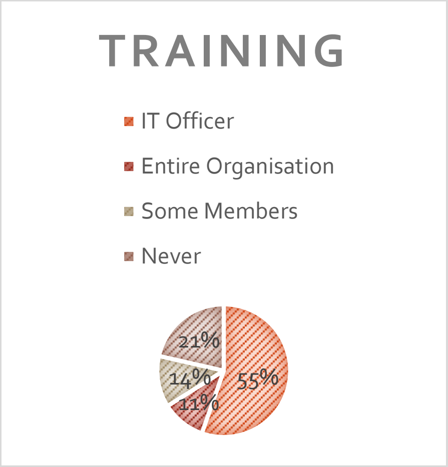
The DSA seeks to pool IT and IT security resources from individuals and organisations to build IT security capacity in the civil society sector

Digital Security Survey

DPI conducted a survey on the state of digital security in civil society. The survey is the background upon which the DSA will fashion strategies for securing information systems and infrastructure for civil society

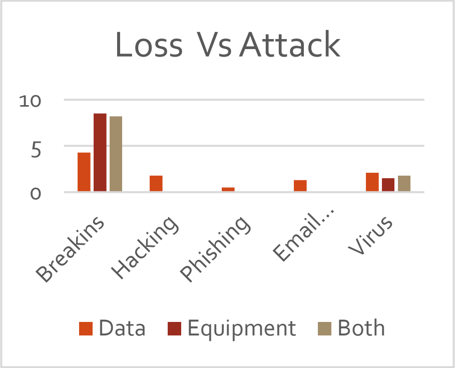
It is evident from the study that there have been efforts to build the capacity of CSOs in digital security through trainings conducted by organisations such as DPI and the private sector





Many of the basic practices have been adopted by trainees in civil society such as installing and updating anti-malware solutions, using strong passwords, data encryption and use of multifactor Authentication, …

Nonetheless there have been several critical weaknesses that have put CSOs at critical risk as evidenced by the nature of attacks they have suffered. These weaknesses include; Office Break-ins, Hacking, Virus attacks, Email Scams, Phishing Campaigns, to mention but a few.



A DPI DSA member explaining to participants in a training workshop to set up 2 step verification

Digital Security Alliance

by Defenders Protection Initiative

The DSA is a coalition of organisations and individual digital security experts working towards securing the digital assets of civil society, human rights defenders, journalists and other activists in the face of threats posed by powerful corporations, unscrupulous criminals, state and other non state actors..

The DSA seeks to pool IT and IT security resources from individuals and organisations to build IT security capacity in the civil society sector.

Our objective

To achieve a safer digital environment for Human Rights Defenders in Uganda by Increasing the capacity of the digital emergency response ecosystem to provide safety for HRD's under attack by covering their digital privacy and digital security aspects including infrastructure security.

DSA aims to close the gap and increase cooperation between civil society, activists on the one side and organizations or individuals working in information security on the other side.

The members of the initiative are a mix between protection providers', NGO project officers and citizens sensitized in freedom of speech and information security. DSA's members donate time and resources to this community in order to globally improve the security awareness of civil society.

DSA will serve as secure proxy to report incidents they have been made aware of and provide information of best practices while protecting its beneficiaries and sources.

DSA wants to build bridges with other response teams and Digital security communities by learning from the best practitioners in the security response field and helping other teams to understand the very specific environment that DSA beneficiaries work.

Constituency

DSA operates thanks to the contributions of its members. Members of DSA contribute with skills and/or with other assets into this initiative. When necessary, DSA will fund-raise to obtain specific access to tools and technologies not available via its members.

Incident response and Proactive services

DSA will assist NGOs or other forms of civil society organizations in handling the technical and organizational aspects of incidents in connection with Digital Security. In particular, DSA will provide assistance or advice with respect to the following aspects of incidents management:

Incident triage

- Establish a secure communication channel with the victims.
- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.
- Help gathering any extra forensic information needed.
- Identifying the best partner or skill set needed to address the incident.

Incident coordination

- Determining the initial cause of the incident.
- Facilitating contact with other organizations that may be involved/affected.
- Providing human readable information for the victims if needed.
- Composing announcements to civil society if applicable.

Incident resolution

- Helping to remove the vulnerability.
- Helping to secure the system from the effects of the incident.
- Identify if the attack is targeted.
- Monitor the persistence of the attackers.
- Collecting evidence of the incident.
- In addition, DSA will collect statistics concerning incidents processed, and will notify the wider community as necessary to assist it in protecting against known attacks.

Proactive services

- DSA coordinates and maintains the following services to the extent possible depending on its resources:
- Secure training for civil society
- Malware analysis
- Information sharing

Activities

Monthly partnership Meetings

The DSA will hold regular monthly meetings at predetermined locations, these meetings will help the partners to keep in touch and updated of arising threats, discuss solutions and share experiences. Also during these meetings, the DSA will collaborate on pending emergency incidents and see how to effectively resolve them

Mentorship and Capacity Building campaigns

The DSA will schedule trainings to build digital security capacity and also mentorship of identified beneficiaries to help them mitigate eminent threats and also educate the identified beneficiary so as to impart good digital ethics to protect and safeguard their privacy

Digital Security performance campaigns

During this activity, different beneficiaries will be identified that the DSA will visit and conduct a digital security health check to asses and examine the capacity, awareness and adoption to proper and safe digital security practices and policies. This will help the DSA to plan and organise relevant digital security training and collaborate relevant solutions within the alliance

Rapid Response

The DSA will offer assistance to any HRD, CSO, NGO and Citizen that is under attack or threat and is in need of emergency or rapid response to help contain or mitigate further damage. In this case the DSA will utilise a ticketing system that will identify the relevant digital security expert depending on the technicalities of the specific security incident.

The Ticketing system can be accessed from http://ticket.defendersprotection.org/

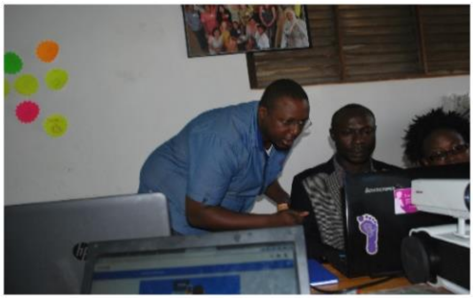
Tools and Application Development

The DSA will innovate, develop and share security tools and technology aimed at preserving privacy and anonymity, circumventing surveillance and equipping the HRD, CSO, NGO or Citizen with skills and best practices.

EMPOWERING CIVIL SOCIETY

Malware Solutions

Install and regularly update anti malware software such as Kaspersky internet Security to provide reliable protection for your computer by making your internet connections, webcam, online shopping safe.



Capacity Building

Regular capacity building for HRD's, CSO's, NGO's and Citizens will help them adopt safer digital security practices and skills.

FAST FACTS

56%

Human rights defenders that have had prior digital security training have been victims of any one digital security attack

54.7%

Civils society organisations do not employ a full time IT professional because they do not have the funds to hire one or do not appreciate the need for one

FOR MORE INFORMATION

in case of an emergency, you can contact

DEFENDERS PROTECTION INITIATIVE
Plot 944, Block 254 Kansanga – Ggaba Road
+256-392-201102
ticketing@defendersprotection.org

http://ticket.defendersprotection.org/

Participants of a digital security training be taken through website security session by DPI Digital Security Executive

Scope of the Digital inSecurity

by Defenders Protection Initiative

A growing number of civil society organizations face many of the same targeted information security threats experienced by governments and the private sector. Some of the same threat actors that make front page news by stealing corporate secrets and infiltrating government computers are also regularly targeting civil society. At the same time, the cost of conducting digital monitoring is dropping and the technologies are being acquired by more government and non-state actors. This leaves open the possibility for these technologies to be further abused and turned against NGOs. Even organizations engaged in work viewed as non-threatening to governments and non-state actors face a more dangerous digital environment due to the rise in cyber-based crime. Despite these developments, digital security risks are not fully understood by many in civil society and organizations often lack the resources to effectively respond.

Types of Digital Security Threats

Digital security threats can be looked at in two ways—**Passive Monitoring**, such as a government tracking a person or an organization's metadata and **Remote Intrusion**, such as the targeted malware attacks discussed above or phishing for purposes of stealing information.

While it can be difficult to demonstrate conclusively that the communications of civil society organizations have been specifically intercepted via passive monitoring (with exceptions), cases of remote intrusion (aka "hacking") have been well-documented. Once an organization has reached a baseline level of digital security against remote intrusion and credential theft, it will be better prepared to address more sophisticated patterns of threats across the board.

Remote intrusion, or targeted attacks, can take a number of forms. For example, civil society organizations are known to be targeted by sophisticated government-linked hacking groups that use advanced intrusion tools. Historically, many of these attacks have begun when victims are tricked into opening a document or link containing malicious code. Once the code has run on the victim's machine, the attackers use this point of entry to collect sensitive information. In other cases, attackers may directly target the computers and servers of organizations looking for weaknesses, such as a lack of software updates, and compromise the device without interacting with victims.

Sophisticated phishing attacks, where victims are tricked into providing passwords or two-factor codes, have also been widely observed targeting civil society groups. These attacks can be highly personalized, and may involve messages masquerading as friends or colleagues of the target.

In addition to direct attacks, civil society organizations can become digitally compromised through interactions with third parties as well. For example, malware infected files can be exchanged between partner organizations, including between a grantee and a funder.

Civil Society's Digital Security Limitations

Despite the growing threats against a range of civil society organizations, many face chronic capacity limits with information technology. These limits are not specific to digital security, but often reflect basic priority-setting by organizations with finite budgets and competing financial pressures. For example:

Many organizations do not have a dedicated IT staff person to manage their computers, network and website.

Often those who do have such a person have not hired someone with experience or competency specifically in information security.

Many organizations also lack basic digital security policies to protect people and data, as well as updated and standardized devices, networked equipment and software.

These capacity limits can translate into security vulnerabilities. Cumulatively, this weakens an organization's overall security plan. These are key areas where the Digital Security Alliance can help drive positive change by opening a conversation with HRDs and CSOs about their overall technology capacity.

Multi-Sector Collaboration Ecosystem

Within civil society, the development of an Multi-Sector Collaboration ecosystem of service providers, non-profit security trainers, advisors and technical tools has emerged as protection organisations work to enhance the digital security of civil society organizations.

However, successful development and deployment of solutions to information security challenges often vary from organization to organization. It is therefore important that all members of the DSA increase their knowledge about information security and how to apply that knowledge in the context of specific organisations.

Improve the Digital Security of your Organisations

Improved digital security should be an aspiration for all civil society organizations, not just those at highest risk. Different organisations will have different levels of risk, below are some questions that you can ask of all organizations to help them improve their digital security.

1. **Question: How is your email hosted?**

Why is this important? Email is a key part of most organizations' operations, yet it can be difficult or expensive to securely manage.

Pitfall to look out for: Self-hosted servers, emails managed on a variety of different platforms, and the widespread use of personal email accounts.

Potential solution: Managed email services for business. Managed solutions improve operational security by outsourcing security concerns to the provider instead of the organization. If organizations host or manage email themselves, be sure they have the internal technical capacity to do so effectively.

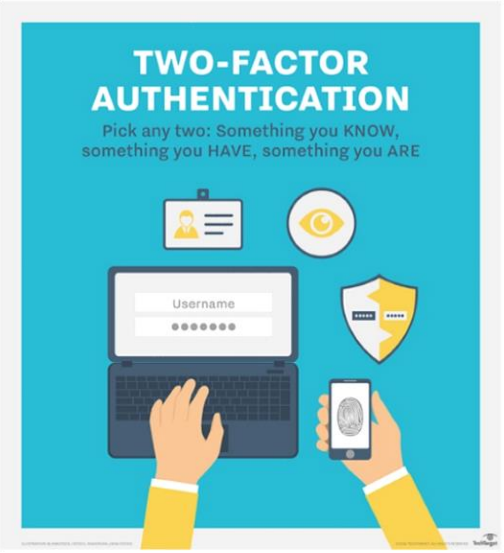
2. **Do you have a policy of "two factor" authentication on work accounts?**

Why is this important? Passwords are a basic security measure, but when used alone are vulnerable to phishing and hacking.

Pitfall to look out for: Lack of additional login security, such as not using two factor authentications (e.g. an authenticator app, tokens, or SMS-based authentication).

Potential solution: Implementing two factor authentication security for organizational accounts. Many service providers such as Google and Facebook offer two-factor authentication as an option waiting to be enabled.

DIGITAL SECURITY TIPS


TWO-FACTOR AUTHENTICATION
Pick any two: Something you KNOW, something you HAVE, something you ARE
Username
•••••••

Two Factor Authentication

Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check

Data Encryption

Data encryption translates **data** into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it.

Data Backups

Backup is the activity of copying **data** to preserve it in case of equipment failure or catastrophes.

Digital Security Tips

by Defenders Protection Initiative

3. Are your devices that store work information encrypted?

Why is this important? Devices should be encrypted so that if devices are lost, stolen, or confiscated, confidential data is protected.

Pitfall to look out for: Lack of "full disk" encryption on devices that handle work information or lack of awareness of the benefits of device encryption.

Potential solution: A policy of full-disk encryption for work devices, including phones and computers, including on any personal devices where work-related information is stored.

4. Do you document digital security incidents?

Why is this important? Mature organizations are likely to have experienced some form of digital security incident during normal operations. Without good documentation, it can be difficult to quickly identify when an incident is occurring, even a large-scale breach.

Pitfall to look out for: Lack of policies and procedures for documenting digital security threats. You can start by asking for post-incident reports from previous attacks or breaches.

Potential solution: We suggest organizations work with an information security expert to establish a basic practice of documenting incidents as this information will be useful to a digital security expert an organization might hire to address a security breach. Such documentation should include, for example, recording suspicious login attempts on accounts, saving suspicious emails, and documenting any loss of control of work devices.

5. Do you have a plan to respond to a crisis (e.g. Do you have a plan for what to do if your email is hacked)?

Why is this important? Suffering a breach can be disruptive and costly, but the costs increase dramatically if there are no plans in place for mitigating the damage and if key information is not regularly backed up.

Pitfall to look out for: Lack of a crisis response plan in case of a breach, lack of backups for data.

Potential solution: Implementing an organizationwide encrypted backup policy, and developing a basic response plan.

6. Does the organization use genuine (non-pirated), up-to-date software and operating systems on computers and mobile devices?

Why is this important? Out-of-date software, or software that is not receiving regular updates are much more vulnerable to malware and other security issues. Pirated software often cannot be updated, and can also come pre-loaded with malicious software.

Pitfall to look out for: Organization is using pirated or un-updated software

Potential solution: Consider acquiring or the purchase of genuine software

In Conclusion Digital security threats are constantly evolving. However, we anticipate that sources of risk and threats, as well as the basic technologies used within civil society, will continue to evolve.

Defenders Protection Initiative
Plot 944, Block 254 Kansanga -Ggaba Rd.
P.O.Box 35864
Kampala – Uganda
Tel: +256 392 201102

Thinking more Systematically

Training is not a silver Bullet

Threats against civil society organizations are serious and can sometimes be highly sophisticated. In some cases, the threat actors targeting civil society organizations are the same groups targeting governments or corporations. In the face of such threats, it would be considered irresponsible by a corporate board or a government oversight body to simply provide a short "digital security training" to employees, without investing in more systematic measures. There is a risk of developing a problem-atic way of thinking about digital security for civil society that results in a separate and unequal approach that is overly weighted towards trainings, and neglects the insights from other sectors that face similar threats.

This can create the problem that recommendations are mismatched with an organization's culture and threats, and, in some cases, create conflicting information and messaging around security issues. Thus, promote faddish security tools, like a secure messaging app that is unlikely to be widely adopted.