



DEFENDERS
PROTECTION INITIATIVE

A Mini Digital Security Handbook for CSOs



www.defendersprotection.org



+256 392 201102



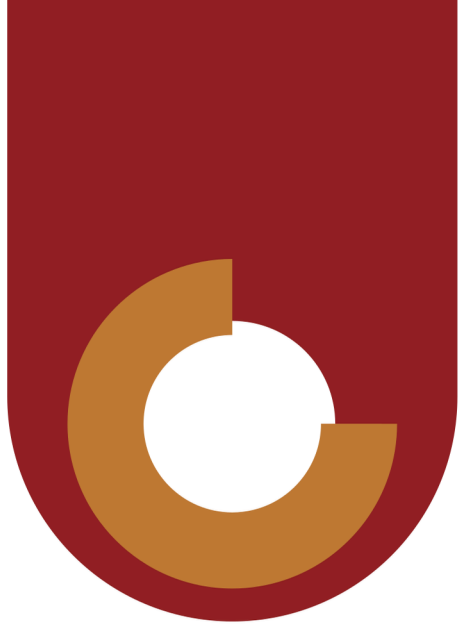


Table of Content

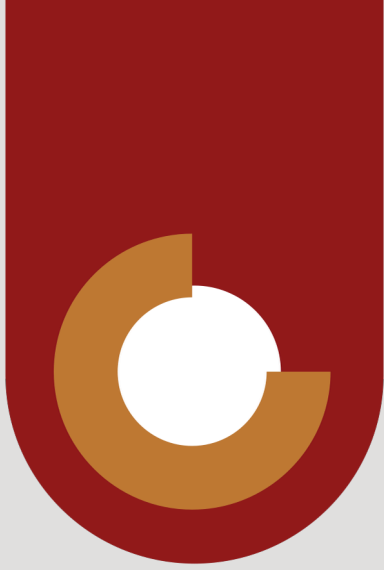
- Introduction.
- Key Definitions.
- Common Digital Security Issues.
- Practical Solutions and Recommendations.
- Tools and Resource
- Building Digital Security Policies.
- Ransomware.
- Appendix: Additional Resources.

1. Introduction

This Mini Digital Security Handbook is developed by Defenders Protection Initiative (DPI), with the support of the National Democratic Institute (NDI), to empower Civil Society Organizations (CSOs) in Uganda with essential digital security skills. As Uganda approaches the 2026 elections, organizations face increasing digital threats, such as surveillance, phishing, malware, and hacking attempts. The contents of this handbook are based on assessments conducted with organizations involved in governance and advocacy work, ensuring it addresses their specific challenges.



The development of this handbook was informed by assessments conducted with CSOs involved in governance and advocacy in Uganda, addressing the specific challenges they face in digital security. As digital threats grow in frequency and sophistication, CSOs must be prepared to defend their digital infrastructure. By implementing the recommendations and tools outlined in this handbook, organizations can significantly improve their security posture. Regular training, strong policies, and the use of cutting-edge digital security tools are crucial for protecting sensitive information, particularly during critical periods like elections.



2. Key Definitions

Digital Security

The practice of protecting digital information, systems, and assets from threats such as cyberattacks, unauthorized access, or theft. For CSOs, digital security is critical for safeguarding sensitive data, such as reports, financial information, and election data.

Encryption

The process of converting information or data into a code to prevent unauthorized access. Encryption protects sensitive communications and files from being intercepted by malicious actors. **Example Tools:** VeraCrypt, PGP Encryption, ProtonMail.

Malware

Malware is malicious software designed to infiltrate and damage systems, steal data, or disrupt operations. This includes ransomware, trojans, viruses, and spyware.

Current Context: Several organizations face regular malware attacks, often through phishing attempts or malicious downloads.

Phishing

A cyberattack that uses disguised emails or messages to trick individuals into providing sensitive information like passwords, or downloading malware.

3. Common Digital Security Issues

Phishing Attacks

Phishing is one of the most common threats CSOs face, where attackers disguise themselves as legitimate entities to steal login credentials or install malware. Often, phishing emails mimic government agencies, donors, or partner organizations.

Recommendation:

Do not click on suspicious links or attachments. Use anti-phishing solutions like Avast and enable spam filtering on all email accounts.

Tools:

- uBlock Origin – Browser extension that blocks malicious scripts.
- PhishTank – A community-based site to check URLs for phishing.



Malware and Ransomware

Malware infects systems to cause damage, steal data, or encrypt files in the case of ransomware. Organizations must take extra precautions to avoid downloading infected attachments or visiting unsafe websites.

Recommendation:

Install reliable antivirus software, use email scanning tools, and ensure that all devices and software are up to date with the latest security patches.

Tools:

- Bitdefender – Provides real-time malware detection.
- Malwarebytes – Scans and removes malware from infected devices.



Weak Passwords and Lack of Authentication

Weak passwords and the absence of multi-factor authentication (MFA) make it easy for attackers to gain unauthorized access to systems.

Recommendation:

Enforce strong password policies, ensure the use of MFA, and store passwords securely in a password manager.

Tools:

- LastPass—A password manager that stores and generates strong passwords.
- Google Authenticator – MFA tool that provides extra login security.
- Authy—MFA tool for extra security.

Surveillance and Monitoring

CSOs involved in governance and election monitoring are at risk of surveillance by third parties, including state actors. This can compromise sensitive communications and lead to the breach of confidential information.

Recommendation:

Use VPNs and end-to-end encrypted communication tools to avoid monitoring and ensure secure communication.

Tools:

- Tor Browser – Provides anonymous browsing to evade tracking.
- Signal – Encrypted messaging app for secure communication.



4. Practical Solutions and Recommendations



1. Securing Communications

Encrypted Messaging:

Ensure that all internal and external communications are conducted through encrypted channels. Tools like Signal and WhatsApp offer end-to-end encryption, protecting your messages from interception.

Recommendation:

Encourage staff to use encrypted apps for sensitive communications and regularly update these tools.

2. Data Encryption and Backup

Data Encryption:

Encrypt sensitive files to prevent unauthorized access. Use tools like VeraCrypt to secure data both in storage and during transmission.

Backup Strategy:

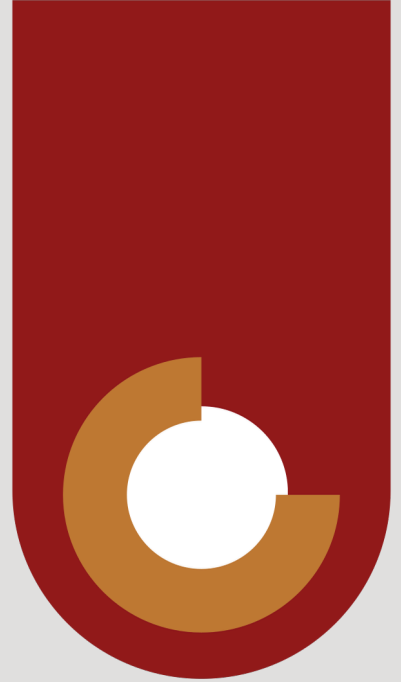
Regularly back up all critical data and ensure backups are encrypted. Store them in multiple locations, including secure cloud platforms and offline storage devices. Adopt secure cloud platforms like Tresorit or Google Drive.

Recommendation:

Adopt a backup routine that includes both daily and weekly backups for critical data.



4. Practical Solutions and Recommendations



3. Safe Internet Browsing

Avoid Public Wi-Fi:

Public Wi-Fi is often insecure, making it easy for attackers to intercept data. If unavoidable, always use a VPN or Tor to secure the connection.

Recommendation:

Limit the use of public Wi-Fi and educate staff on the risks of using insecure networks.

4. Incident Response Plan

Develop a digital incident response plan that outlines steps to take when a breach or cyberattack occurs. This should include:

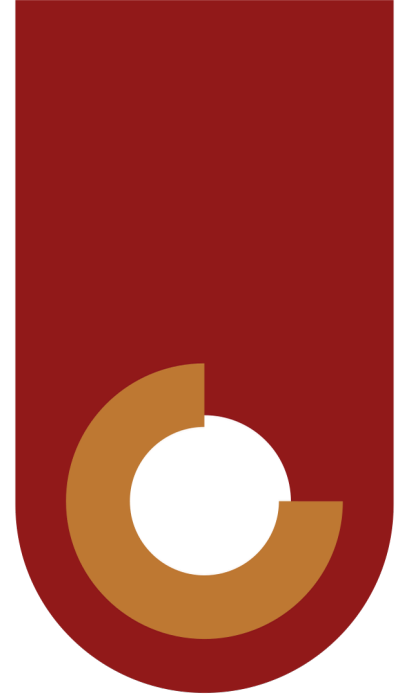
1. Immediate isolation of infected devices.
2. Notification protocols for internal and external stakeholders.
3. Data recovery from backups.

Recommendation:

Regularly test your incident response plan through simulations.



4. Practical Solutions and Recommendations



5. Training and Awareness

Regular digital security training should be provided to staff to keep them updated on the latest threats, such as phishing attacks, malware, and ransomware. Awareness campaigns help reinforce best practices.

Recommendation:

Conduct regular training sessions and refresher courses for staff.

4. Tools and Resources



Encryption Tools

- • **Signal** – Secure messaging app with end-to-end encryption.
- **WhatsApp** – Provides encrypted messaging for private communications.

VPN and Anonymity Tools

- • • **ProtonVPN** – High-quality VPN that ensures private browsing.
- **Orbot** – A multi layer privacy based tool to anonymize your browsing experience.
- **Tor Browser** – A browser that anonymizes web traffic, protecting your identity online.

Antivirus and Malware Protection

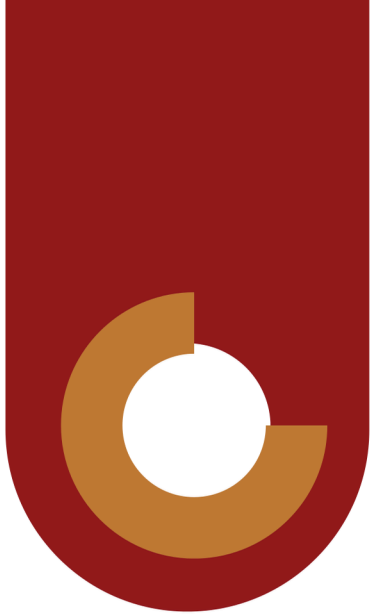
- • • **Bitdefender** – Offers comprehensive protection against malware, ransomware, and other cyber threats.
- **Kaspersky** – Known for its robust malware detection and protection capabilities.
- **Kaspersky Cloud** – A free alternative for Kaspersky antivirus.

Password Management and Authentication

- • **1Password** – Password manager for storing and generating strong passwords.
- **Google Authenticator** – Adds a second layer of authentication for account security.

Backup Solutions

- • **Tresorit** – Offers secure, encrypted backups for critical data.
- **Google Drive with Encryption** – Cloud-based backup solution with encryption options.



6. Building Digital Security Policies

Every organization must have a digital security policy to govern its practices and protect its assets. These policies should cover areas such as:

- Password management
- Data encryption
- Use of secure communication tools
- Incident response planning

How to Build a Digital Security Policy:

1. **Assess Risks:** Identify key vulnerabilities in your digital infrastructure and classify your sensitive assets.
Develop Guidelines: Create rules for data management, password usage, encryption, and secure communication.
2. **Use Templates:** Platforms like [usesoap.app](#) offer customizable templates for building comprehensive digital security policies.
3. **Regular Review:** Ensure policies are reviewed and updated periodically to address new threats
- 4.

7. Ransomware



What is Ransomware?

Ransomware is a type of malware that encrypts a victim's files, demanding payment in exchange for the decryption key. It often spreads through phishing emails or malicious software downloads.

Prevention and Response:

1. **Regular Backups:** Ensure all critical data is backed up and stored securely.
Email Vigilance: Avoid clicking on unknown attachments or links from unverified sources.
2. **Network Segmentation:** Limit the spread of ransomware by isolating sensitive systems from general networks.
- 3.

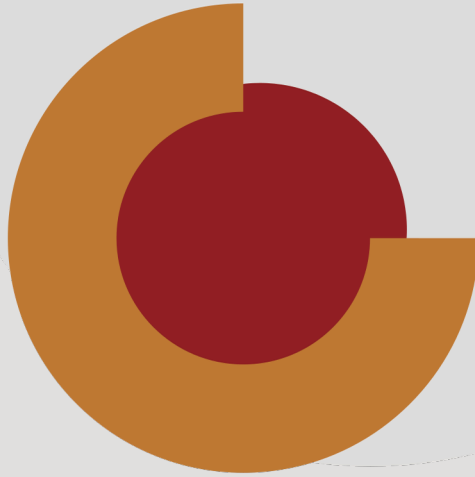
Relevant Tools:

- **Bitdefender Anti-Ransomware** – Protects against known ransomware types.
- **Cloud Backup** – Allows for the secure restoration of files without paying the ransom.

8. Appendix:

Additional Resources

- [DigitalSecurity.io](#) – Online courses on encryption and cyber resilience.
- [Security.org](#) – Comprehensive cybersecurity resources for nonprofits and advocacy organizations.
- [CyberPeace.org](#) – Tools and guides on staying safe online.
- [usesoap.app](#) – A tool for building customized digital security policies.
- [HaveIBeenPwned.com](#) – Check if your email has been involved in a data breach.
-



9. Contact Us

Website: www.defendersprotection.org

X: @defprotection

Email: communications@defendersprotection.org

Tech Support: ict@defendersprotection.org

Signal: @DPI.03

