Amnewswatch

# DIGITAL SAFETY & ENLIGTHMENT TOOLKIT

By

## AMNEWSWORLD

Prepared for
Digital Storytellers

*Your guide to safer online practices, threat reporting, and digital resilience.*

## 1. Introduction

Welcome to the Amnewswatch Digital Safety Toolkit!

In today's world, digital tools connect us, inform us, and empower us but they can also expose us to risks like scams, cyberbully, and misinformation.

This toolkit is here to help you:
-Stay safer online
- Understand digital threats
- Build long-term habits for digital resilience
- Know what to do and who to contact when things go wrong

Use it as a personal guide, share it with your family, or train your team or community with it.

## 2. Cyber Hygiene Essentials

- ✓ Use strong passwords: Mix uppercase, lowercase, numbers, and symbols.
- ✓ Don't reuse passwords. Consider using a password manager.
- ✓ Turn on Two-Factor Authentication (2FA): This adds an extra layer of security
- ✓ Browse with care: Look for the padlock symbol. Avoid suspicious links.
- ✓ Keep devices updated: Updates fix security issues.
- ✓ Use antivirus software: Many good free options exist.

## 3. Recognizing Digital Threats

- ✓ Phishing emails & messages: Don't click links or share info unless you're sure it's legit.
- ✓ Misinformation & fake news: Watch for shocking headlines, poor grammar, emotional manipulation.
- ✓ Social media impersonation: Verify unusual behavior from contacts asking for money or help.

## 4. Responding to Digital Incidents

Act fast, don't panic.

If your account is hacked:
- Change your password
- Log out of all sessions
- Turn on 2FA

- Report to the platform

If you encounter a threat:
- Report it to Amnewswatch
- Block or mute the attacker
- Take screenshots and keep evidence

Template: Reporting a Threat
Hello, I'd like to report [type of threat: scam, abuse, impersonation, etc.]. It occurred on [platform] and involved [brief description]. I've attached screenshots and can provide more info if needed. Thank you.

### 5. Building Digital Resilience

✓ Check your privacy settings: Review who sees what on your social media.

✓ Teach others: Share this toolkit with others, especially those less tech-savvy.

✓ Learn continuously: Subscribe to security newsletters, join webinars, or follow trusted sources like Amnewswatch.

### 6. Quick Tools & Resources

Helpful Tools:

-Credential Manager: https://www.phoxtra.com/
- Password Manager: https://bitwarden.com/
- 2FA Guide: https://2fa.directory/
- Malware Scanner: https://www.malwarebytes.com/

Trusted Fact-Checkers:
- Africa Check: https://africacheck.org
- Snopes: https://snopes.com
- Google Fact Check Explorer: https://toolbox.google.com/factcheck

Threat Reporting:
- Report a Threat to Amnewswatch
- Contact our team → [Insert link]

About Amnewswatch

Amnewswatch is committed to advancing digital safety, countering misinformation, and empowering individuals and communities with practical knowledge for online resilience. We monitor digital trends, provide timely reporting tools, and build awareness to ensure safer digital spaces across Africa and beyond.

## Digital Surveillance & Freedom of Expression

In an increasingly digital world, surveillance technologies are often used to monitor, track, and sometimes silence voices online—particularly journalists, bloggers, and content creators. While some monitoring is done in the name of security, unchecked surveillance can threaten digital rights and press freedom.

### What is Digital Surveillance?

Digital surveillance refers to the use of technology to monitor activities, communications, or behaviors online. This includes:

- ✓ Monitoring emails, chats, and social media posts
- ✓ Tracking location via mobile or IP addresses
- ✓ Using spyware or malware to access devices
- ✓ Collecting metadata on browsing habits

For **journalists, bloggers, and content creators**, this can lead to:

- ✓ Self-censorship due to fear of retaliation
- ✓ Harassment or arrest for exposing truths
- ✓ Invasive monitoring without consent

### How to Stay Protected

- ✓ While no tool is 100% secure, here are some ways to minimize risk:
- ✓ Use encrypted communication tools (e.g., **Signal**, **ProtonMail**)
- ✓ Use VPNs when accessing sensitive content or conducting investigations
- ✓ Avoid storing sensitive sources or notes on cloud services without encryption
- ✓ Regularly update and scan devices for spyware or monitoring tools
- ✓ Be aware of phishing and impersonation targeting you or your sources

## Enhancing Digital Freedom Responsibly

Digital freedom is not just about evading surveillance—it's also about **building a trusted and informed digital community**.

**Verify before you publish**: Use fact-checking tools to avoid spreading misinformation.

**Be transparent**: Explain your sources and intentions when reporting online.

**Support others**: Defend voices under threat and share tools for safe expression.

**Promote media literacy**: Educate audiences about how misinformation spreads and how to critically evaluate information.

---

> ***"We encourages all digital storytellers to use their voice boldly but also safely.*** *By promoting digital safety, ethical content, and informed communities, we can resist misuse of surveillance and safeguard our freedom of expression".*

This toolkit was developed to support individuals, families, educators, journalists, and civic leaders in protecting themselves and others in the digital space.

For more resources or to get in touch, Contact Amnewswatch.