DIGITAL SECURITY TRAINING MANUAL

FOR STRUCTURALLY SILENCED WOMEN IN UGANDA

WOMEN AND ICTS
WOMEN OF UGANDA NETWORK
WOUGNET

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Authors: Gole Andrew, Ruth Atim, Sandra Aceng and Patricia Nyasuna

Design: Gole Andrew

On Behalf of Women of Uganda Network (WOUGNET)

Table of Contents

Preface

Structurally silenced women ought to be safe and able to advocate for their rights online and offline without any slight fear of being attacked or harassed.

The increased usage of digital technology and online platforms has made the internet become a cherished resource for all women,' especially structurally silenced women such as LBT and sex workers, WHRDs, young women, those living in rural communities or from historically excluded counties, and districts, and those across constituencies and identities.

Much as they have embraced the usage of digital technologies, there is a need to have a document that they can always refer to, especially when the need to do digital security training arises.

It is on this note that WOUGNET under the Our Voices, Our Futures (OVOF) project developed a Digital security training manual tailored for Structurally silenced women to support them with basic digital safety information that they can use in-house and out.

Acknowledgements

This digital security manual is a curation of different digital security tips and best practices for ‘all women,’ especially structurally silenced women such as LBT and sex workers, WHRDs, young women, those living in rural communities or from historically excluded counties and districts, and those across constituencies and identities.

It was developed to avail information on digital safety and possibilities to use digital technologies for collectivization and advocacy based on the findings from research conducted nationwide under the Our Voices, Our Futures (OVOF) Project which was implemented by Women of Uganda Network (WOUGNET) with support from the Association for Progressive Communications (APC).

Acronyms

2FA	2 Factor Authentication
ADIDS	Activity, Discussion, Input, Deepening, and Synthesis
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LBT	Lesbian, Bi-sexual, and Transgender
MALWARE	Malicious Software
NCII	Non-consensual Sharing of Intimate Images
OGBV	Online Gender-based Violence
PIN	Personal Identification Number
USB	Universal Serial Bus
WOUGNET	Women of Uganda Network
WWW	World Wide Web
WHRDs	Women Human Rights Defenders

Glossary

Anonymity	When the real author of a message is not shown.
Attacker (or Adversary)	Someone that wants to undermine your security goals.
Cipher text	Encrypted text. Plaintext is what you have before encryption, cipher text is the encrypted result.
Decryption	The act of combining cipher text and a key to convert it back to plain text.
Encryption	This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
Information Security	A process of maintaining confidentiality, ensuring integrity and assuring availability of data you want to protect.
Ransomware	A malicious software that requires the victim to pay a ransom to retrieve access to files encrypted by the malware.
Server	A computer that makes services, as access to data files, programs, and peripheral devices, available to workstations on a network.

Spyware

A software that secretly gathers information about a person or organization and that is designed to take partial or full control of a computer's operation without the knowledge of its user.

Spoofing

A fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

Virus

A type of malicious software program that, when executed, replicates itself by modifying other computer programs and inserting its own code.

Wi-Fi

The name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connection.

Wi-Fi/Router:

A device that is used to provide access to the Internet or a private computer network.

Whaling

A specific form of phishing that's targeted at high-profile business executives, managers, and the like.

About the Manual

WOUGNET in collaboration with Association for Progressive Communications (APC) are implementing the Our Voices Our Futures (OVOF) project which seeks to change the situation of 'all women,' especially structurally silenced women such as LBT and sex workers, WHRDs, young women, those living in rural communities or from historically excluded counties and districts, and those across constituencies and identities.

It is upon this background that in November 2021, WOUGNET conducted a Digital Security Needs Assessment on the digital security needs of activists and organizations in the specific groups of structurally silenced women which included; Sex Workers, LBT, WHRDs, feminists and activists organizations, and individuals. The groups were sampled from districts of; Kampala, Wakiso, Gulu, Kamwenge, Lira, and Arua.

The objectives of the Needs Assessment were as follows;

- Understand the impact of digital technologies on structurally silenced women to support them accordingly.
- Increase the use of digital technologies safely and securely.
- Avail information on digital safety and possibilities to use digital technologies for collectivization and advocacy.
- Build and/or strengthen skills, analysis, and networks to use and influence development and policymaking related to digital technologies.

The needs assessment discovered a number of challenges these categories of women face online but also developed recommendations from participants of the assessment. These include; Limited knowledge in using the technology and its latest trends including social media, online bullying (trolling & sexual harassment), online scams or fraud that has limited their usage of other technology features like online banking, lack of privacy due to public computers, Data protection, and security issues.

This digital security training manual was developed to aid in the training of structurally silenced women on how they can protect themselves from the common threats they face online. The manual is made simple so that it can be useful to both technical and non-technical persons. This manual is intended to be used to offer digital security trainings for LBT women, Sex Workers, WHRDs, and other structurally silenced women.

Structure of the Manual

The manual has 6 structured sections that provide basic digital security skills, tools, and techniques that can be used by structurally silenced women to improve their safety online.

These sections include;

- Section 1: Understanding Digital Security.
- Section 2: Threat Modelling & Risk Assessment.
- Section 3: Online Security.
- Section 4: Password Management.
- Section 5: Secure Communication.
- Section 6: Device Management & Hygiene.

Section 1: Understanding Digital Security

Digital Security is the protection of one’s digital personality and assets as it represents one's physical identity offline. Digital Security includes the tools which one uses to secure his/her/other identity, assets, and technology in the online and mobile world.

1.1. Digital Security for Structurally Silenced Women.

Having the right digital skills and techniques can ensure that women have a better chance to take charge of their digital safety online. However, adoption of digital security skills is still low amongst vulnerable groups like structurally silenced women because of several common myths and misconceptions. Below are some of these myths and misconceptions;

- Our organization is too small to be a victim of a cyber attack
- Anti-virus/Anti-malware is good enough.
- Our passwords are strong.
- Threats are spread only through the Internet.

1.2. Improving the Digital Security of Structurally Silenced Women.

The internet provides an opportunity to stay anonymous, while simultaneously allowing access to the privacy of its users. The accessibility and nature of online services also means that abuse can be done remotely. Structurally silenced women have been victims of digital insecurity. In this section, we explore ways of improving their state of digital Security.

Section 2: Threat Modelling and Risk Assessment.

2.1. Introduction to Threat Modelling and Risk Assessment

Risk Assessment is a way of identifying and managing potential threats that could harm, damage, and disrupt digital assets. For structurally silenced women to take charge of their online security, they need to conduct a risk assessment to help them know their threat model. This involves thinking critically about the digital security threats they are exposed to so as to enable them develop personalized strategies to mitigate those risks.

Examples of Online Threats and Vulnerabilities

Structurally silenced women are faced with several digital security threats and vulnerabilities and this has limited their use and adoption of digital platforms. These threats have unique negative effects on the lives of these women especially LBT women, sex workers, WHRDs, and other groups of women.

Some of the online threats faced by these structurally silenced women include; Cyber-stalking, Trolling, Doxxing, Cyber-bullying, Impersonation, Hate Speech, Public Shaming, Non-consensual Sharing of intimate images (NCII), and Online harassment among others.

2.2. Security Plans, Policies, and Protocols

Security planning helps you to identify what could happen to the things you value and determine from whom you need to protect them. The following five questions need to be answered; What do I want to protect?; Who do I want to protect it from?; How bad are the consequences if I fail?; How likely is it that I will need to protect it?; How far am I willing to go to try to prevent potential consequences?

Question 1: What do I want to protect?

These are called assets, for example, your emails, contact lists, instant messages, location, and files are all possible assets. Your devices may also be assets.

Security Tip 1: Make a list of your assets: data that you keep, where it's kept, who has access to it, and what stops others from accessing it.

Question 2: Who do I want to protect it from?

These are adversaries (persons or entities that pose a threat to your assets). Examples of potential adversaries are your boss, your former intimate partner, your business competition, your government, or a hacker on a public network.

Security Tip 2: Make a list of your adversaries, or those who might want to get a hold of your assets. Your list may include individuals, a government agency, or corporations.

Question 3: How bad are the consequences if I fail?
There are many ways that an adversary could gain access to your data. For example, an adversary can read your private communications as they pass through the network, or they can delete or corrupt your data.

Security Tip 3: Write down what your adversary might want to do with your private data.

Question 4: How likely is it that I will need to protect it?
These are risks, the likelihood that a particular threat against a particular asset will actually occur. It goes hand-in-hand with capability.

Security Tip 4: Write down which threats you are going to take seriously, and which ones may be too rare or too harmless (or too difficult to combat) to worry about.

Question 5: How far am I willing to go to try to prevent potential consequences?
There is no perfect option for security. Not everyone has the same priorities, concerns, or access to resources. Your risk assessment will allow you to plan the right strategy for you, balancing convenience, cost, and privacy.

Security Tip 5: Write down what options you have available to you to help mitigate your threats.

Section 3: Online Security.

3.1. Understanding Online Security.

Online security are the rules that structurally silenced women should follow, take actions, and processes that happen to ensure that they are safe on the Internet. With security threats (malware, scams, phishing, hacking, etc.), online security has become more important than ever.

.

Overview of the Types of Online Security.

Talk about the various forms of online security. You can talk about the following;

- Application Security
- Denial-of-Service Attacks
- Man-in-the-Middle Attack
- Password Attack, etc.

3.2. How to Protect Online Accounts and Resources.

We are going to look at several useful techniques that can be put in place to ensure online resources and accounts are protected from online threats and attacks.

3.2.1. Introduction to Safe Browsing Practices.

It's important to practice safe browsing in order to protect online accounts and resources. There are tools and techniques in place that can help in ensuring that we browse safely.

Section 4: Password Management.

Passwords are the first line of defense for information in any form. Best password strength and other key practices evolve over time depending on behavior and the formation of various threats.

It is very important for structurally silenced women to practice proper password management etiquette in order to secure their data and devices. A great password can boost the safety and security of data and information.

4.1 General Password Management

Under password management, we will look at why passwords are important, the characteristics of a good password, and how to create and store passwords using password managers.

Why Passwords are very important.

- Passwords provide access to a number of crucial important accounts such as email, banking accounts, social networking sites, etc.
- Passwords also provide access to Wi-Fi, access points, mobile devices, computers, decrypting of devices, files, and more.

12 Useful Password Management Tips

- Use a unique password for each of your important accounts (i.e. email and online banking). Do not use the same password across multiple accounts.
- Your password should be at least 8 characters long. Passwords should consist of lowercase and uppercase letters, numbers and symbols.

- Do not use personal information such as your name, age, date of birth, child’s name, pet’s name, or favorite color/song when constructing your password.
- Avoid consecutive keyboard combinations (i.e. qwerty or asdfg).
- Look around and make sure no one is watching while you enter your password. If somebody is, politely ask them to look away.
- Always log off/sign out if you leave your device for the day – it just takes a few seconds to do this and it’ll help ensure that no one uses your system for malicious purposes.
- Avoid entering passwords on computers you don't control – they may have malicious software installed to purposely steal your password.
- Avoid entering passwords when connected to unsecured WI-Fi connections (like at an airport or coffee shop) – hackers can intercept your passwords and data over unsecured connections.
- Never tell your password to anyone.
- Change your passwords regularly and avoid using the same password over and over again.
- Never write down your passwords on sticky paper and hide them underneath your workstation or telephone. Somebody will find it.
- Always select “never” when your Internet browser asks for your permission to remember your passwords.
- Make your password easy for you to remember and hard for others to guess hence making it practical.

6 Characteristics of a Strong Password

- Contain at least 8 characters—the more characters, the better.
- Contain a mixture of both uppercase and lowercase letters.
- Contain a mixture of letters and numbers.
- Contain special characters, e.g., ! @ # ?] Note: do not use < or > in your password, as both can cause problems in Web browsers.
- Created from passphrases that make it easy for you to remember but hard for someone else to guess. For example, Let's have lunch at 1:00 p.m. becomes Lh!@1:00 p.m.
- Changed regularly and not used across multiple sites.

4.2. Introduction to Password Managers

A password manager is essentially an encrypted digital vault that stores secure password login information you use to access apps and accounts on your mobile device, websites, and other services.

In addition to keeping your identity, credentials, and sensitive data safe, the best password managers also have a password generator to help you create strong, unique passwords and ensure you aren't using the same password in multiple places.

Examples of Password Managers

- LastPass.
- Dashlane.
- 1Password.
- KeepassXC.
- Bitwarden.
- LogMeOnce.

Characteristics of Good Password Managers

- Password generator.
- Password strength reports.
- 2-factor / Multi-factor authentication.
- Auto-fill web forms.
- Password management for apps.
- Automated password change features.
- Password syncing across multiple devices.
- OTP(One Time Password) generator.

Practical Demonstration: How to Install and use LastPass.

For this demonstration, we will look at LastPass and its key features. After this, we will do a step-by-step guide on how to install and configure LastPass Password Manager. It is also available for downloading from Play Store and App Store.

Key Features of LastPass.

- All the information (passwords, secure notes, credit card numbers) in your LastPass "vault" is encrypted and the only way to access it is via your master password.
- Nobody — not even the people at LastPass — can access your vault without your master password.
- LastPass auto fills your passwords so you never have to type them in again.
- All of your passwords are automatically synced between all your devices where you have LastPass installed. That way, you can access your passwords anywhere.

Installation of LastPass.

1. To install the LastPass Application on your computer, go to lastpass.com and download the application. LastPass is a paid application but you can use the free version for non-commercial work.
2. On the website, you will be prompted to create an account. Follow the steps to create an account. During account creation, you will be prompted to create a master password so be sure to make it strong, strength metre is there to guide you.
3. On clicking ‘create account’, you will receive an email and also be prompted to install the browser extension for the browser that you are using.
4. After installing the browser extension, open it up and be sure to read and accept the terms and conditions.
5. After that, you will be prompted to log in to your LastPass account and that's it.

Add a password to LastPass by logging in to a site

1. In your web browser toolbar, click the inactive LastPass icon.
2. Enter your email address and master password, then click **Log In**.
3. In your web browser, navigate to your desired site.
4. Enter your username and password for the site and proceed to log in.

When prompted by LastPass, click **Add** to add the site entry to your Vault.

Add a Password while in your LastPass Password Vault

1. Log in to LastPass and access your vault by doing either of the following:
    - In your web browser toolbar, click the LastPass icon and select **Open My Vault**.
    - Go to https://lastpass.com/?ac=1 and log in with your email address and master password.
2. Select **Passwords** in the left navigation.
3. Click the Add icon.
4. Enter the URL of the site, and all other information you want to store. You can also select a folder to store it within. If desired, click **Advanced Settings** and enable the checkbox(es) for additional security options of **Require Password Reprompt**, **Autologin**, and/or **Disable Autofill**.
5. Click **Save**.

Section 5: Secure Communication

Secure communication is an important step in ensuring that we boost our digital security and it involves preventing unauthorized access to communication and information being shared between different people. Under secure communication, we will look at email security and secure text messaging.

5.1. Basic Email Security

Email security focuses on the different methods and techniques put in place to protect sensitive information shared through email and this involves protecting the email accounts against unauthorized access which can lead to loss of access or compromise of the information being shared.

How to Secure Email Accounts

Using 2-Factor Authentication

2-Factor Authentication is a technique that involves adding a second means of verifying that you are the owner of the email account in addition to the email password. This method adds a second layer of protection like receiving verification codes through text messages, automated phone calls, or using a security key (a device that is with you all the time).

Using Email Encryption

Email encryption is a way of disguising the contents of an email message to prevent sensitive or confidential information from being read by someone else other than the intended recipients.

Importance of Email Security.

- To prevent phishing attacks.
- To prevent malware attacks.
- To avoid identity theft.
- To protect confidential/ sensitive information.
- To avoid financial fraud.

Common Email Security Best Practices.

1. Always check your email activity and settings.
2. Do not use the same password for different email accounts.
3. Don’t forget to log out every time you sign in to your email account.
4. Regularly change passwords for your email accounts.
5. Never open attachments or links in your emails unless you know and trust the source of the links are shortened you can always use the link unshortener to see the kind of link is shared such tools can be;

- https://unshorten.it/
- https://unshorten.me/
- https://linkunshorten.com/

6. Use email encryption should you need to share confidential/ sensitive information via email.

Practical Demonstration 1: Activating 2-Factor Authentication on Google Account

Google’s 2FA feature will help keep your account safe and secure. If someone tries to sign in to your Gmail account from a device you've never used before, Google will then require them to enter a security code obtained via text message or a mobile authentication app along with your password.

1. Open your Gmail app, select your account and click on **Manage Your Google Account**.
2. Scroll to the right and select the option **Security** in the menu as shown below.
3. Scroll down and tap **two-step verification**, Google's name for two-factor authentication.
4. You'll then see a brief explanation of the feature. Tap **Get Started.**
5. Your first option is to let Google send prompts to your phone asking you to approve a sign-in on another device. This is one of the better ways to do 2FA. Tap **Continue**.
6. As a backup option, Google wants your mobile phone number to help you get access to your account if the first 2FA option fails. You can choose between receiving a one-time passcode via a phone call or by text message. (The phone call is more secure.) Choose one and tap **Send.**
7. Google will call or text you a one-time code. Enter the code sent to your device and tap the **Next** button once that’s done.
8. All you have to do now is to click **Turn on** to finish the process and activate the feature.

Practical Demonstration 2: Activating 2-Factor Authentication for Facebook Account.

- Step 1: Login to Facebook.
- Step 2: Go to your Security and Login Settings.
- Step 3: Scroll down to Use two-factor authentication and click Edit.
- Step 4: Choose the security method you want to add and follow the on-screen instructions.
- Step 5: Select or add a phone number to use.

5.2. Secure Messaging

Messaging is the form of sending communication through a digital device or platform in the form of text or audio. There are very many messaging applications in use today and we will look at some of them and see which ones are more secure and good for sending confidential and sensitive information.

Examples of Messaging Applications.

- WhatsApp Messenger
- Facebook Messenger
- Signal Private Messenger
- Telegram
- Wire
- iMessage
- Viber

Important Features of Secure Messaging Applications.

- **Support end-to-end encryption:**

When you send messages via secure applications, only the intended recipient can read the message. Third-party services providers, application developers, or the government cannot read the contents of the message.

- **Records of Conversation not stored:**

Secure messaging applications like Signal do not store records of chats on the server.

- **User Data not Collected or Stored:**

Secure Messaging applications do not collect, store or sell user data to third-party advertisers.

- **Open Source:**

Secure messaging applications like Signal are run by not-for-profit organisations and therefore are mostly open-source which gives security experts the chance to audit the source code.

Signal Private Messenger: Why it's a better secure messaging option than WhatsApp.

The signal is a private messaging app, which doesn't just offer end-to-end encryption, but also offers privacy-oriented features and collects minimal user data. Here's a quick look at five privacy features offered by the messaging app.

Ability to Block Screenshot

With Signal Private Messenger, you can restrict users from taking screenshots of chats or any other thing within the app. Since it's a privacy-focused instant messaging app, Signal offers this feature so that no one can gather information via screenshots without your consent. To enable the feature, tap on the three dots, and select Settings. On the Settings, tap on the Privacy, and enable the 'Screen Security' feature.

Blur Faces

Signal Private Messenger also has a unique feature that allows you to protect your identity. If you often share your images with others but feel unsafe, you can utilise the Blur feature. To blur Faces on the Signal app, select the picture and tap on the 'Blur' icon located on the top.

Send Disappearing Messages

Disappearing Messages or Self-destructing messages is a must-have for all private and secure messaging apps. Signal also has a disappearing message feature, which makes a message disappear after the recipient has read it. To send disappearing messages, open a chat, and tap on the 3-dot menu. From the list of options that appears, select 'Disappearing messages' and set the timer.

Setup Screen Lock

Screen Lock is a feature that makes the app more secure as you will need to access the app through a PIN or Fingerprint lock. To set up a screen lock in the Signal app, head to the Settings > Privacy > Toggle Screen lock to On.

Send One-time Viewable Image

Signal Private Messenger has a unique feature that allows you to send images that can be viewed only once. Once viewed, the image will disappear from both ends. Just open the picture and tap on the ‘infinite icon’ located at the bottom to use this feature. Tap on it to chat it to ‘1x’. Once done, send the image, and it will be auto-deleted after it’s viewed once.

Getting Started with Signal Private Messenger: A Step-by-Step Guide

Signal is an end-to-end encrypted instant messaging app but with a lot more focus on user security and privacy.

Step 1: Download Signal for Android | Download Signal for iOS.

Step 2: Once you download and open the app, you will be presented with the app’s terms & privacy policy. Ensure you go through it carefully and hit CONTINUE afterward.

Step 3: Next, you would need to grant some permissions: Audio, Contact, Camera, etc. You also do need an active phone number (based on your country of residence) to sign up. A verification message will be sent to the number before sign-up can be completed.

Step 4: Once verification is complete, you will then need to set up your user profile. Here, you need to provide a first name but the last name is optional. Adding a profile picture is optional as well.

Step 5: It is also mandatory to create a 4-digit pin to secure your account. Once that is done, you will then be taken to the home page of the Signal app.

Step 6: To send a message on Signal, click on the **pencil icon** at the bottom-right corner of the screen. A list of all your contacts using the Signal app will appear. Select the contact you want to text and proceed to type your messages, send media files, make voice & video calls, etc.

Step 7: For extra security and privacy, you can customise a sent message to disappear after a certain amount of time. To set and send disappearing messages, click the three-dot icon at the top-right corner of the chat page and select **Disappearing messages**. Next, set the time you want the message to disappear and click **OK**.

Conclusion:

Signal basically works like any messaging app and if you have WhatsApp, Messenger, or Telegram, it comes with some familiar chat features, so you shouldn't have a hard time using the app. The standout and most important benefit of Signal, however, is the privacy-centric features.

Section 6: Device Management and Hygiene

Device management involves managing the implementation, operation and maintenance of digital devices and related applications/software. It includes various administrative tools and processes for the maintenance and proper functioning of a digital device/ equipment.

Under Device management, we will focus on two aspects:

- Device Security and Malware Protection.
- Safer Software Updates and Practices.

Regardless of your broader objectives, keeping your device healthy is a critical first step down the path toward better security. Before worrying too much about data encryption, private communication, and anonymous browsing, for example, you should protect your device from malicious software.

6.1. Device Security and Malware Protection.

Under device security, we will look at the common tools and techniques that can be used to boost the security of our devices which range from Laptops, Smartphones, Desktops, Smart Watches, Digital Cameras, etc. It is important to ensure these devices are digitally secure because they store a lot of data/ information which could be catastrophic if it falls in the wrong hands. Also, many digital devices are connected to the internet and this makes it very easy to compromise them if proper measures are not put in place to protect them.

Common threats faced by Digital Devices.

- Physical theft of digital devices and equipment.
- Malware attacks e.g Virus Attacks, Ransomware Attacks, Trojan Attacks, etc.
- Device physical damage due to poor handling.
- Device failure due to reaching its end of life period.
- Data leaked by the device repairers.
- Data leaked by children playing with the phone/device.

Seven Basic Security Tips for Windows Devices .

There are some ways to beef up your computer's security, and many of them won’t cost you a dime. Below is a quick summary of what to check, and what you can do to improve your security;

- Keep Windows up to date.
- Set a log-in password if you haven’t already done so.
- Consider additional sign-in options. Windows 10 has Dynamic Lock, which lets you pair your computer to your smartphone via Bluetooth, and then automatically locks your computer whenever you carry your smartphone out of range. It's available through Settings > Accounts > Sign-In Options.
- Make sure your antivirus software is running and up to date.
- Make sure other users don’t have Administrator privileges.
- Keep applications updated and uninstall software you never use.
- While using windows set up bios password and disable USB ports on startup to block people from booting your computer using a live boot install.

While you’re at it, consider tightening up your privacy. Explore Settings > Privacy and consider making changes such as these;

- Switch off your location.
- Switch off your Microsoft Advertising ID.
- Tell Windows not to send your Activity History to Microsoft.
- Don’t use Diagnostics & Feedback data for marketing.

Five Security-Related Settings for Android Mobile Devices.

Access To Your Phone

Enable Lock SIM card, found under Settings -> Personal -> Security -> Set up SIM card lock.

Set up a Screen Lock, found under Settings -> Personal -> Security -> Screen Lock, which will ensure that a code, pattern, or password needs to be entered to unlock the screen once it has been locked.

Network Settings

Turn off Wi-Fi and Bluetooth by default. Ensure that Tethering and Portable Hotspots, under Wireless and Network Settings, are switched off when not in use. Settings -> Wireless & Networks -> More -> Tethering & Mobile Hotspot.

Software Updates

The phone operating system: go to: settings -> About phone -> updates -> check for updates.

Apps you have installed: Open the Play store app, from the side menu select My Apps.

Device Encryption

This can be done in Settings -> Personal -> Security -> Encryption. Before you can utilise device encryption, however, you will be required to set a screen lock password.

Location Settings

Switch off Wireless and GPS location (under Location Services) and mobile data (this can be found under Settings -> Personal -> Location).

Five Security-Related Settings for Apple Mobile Devices (iPhones)

Have A Strong Passcode

Go to Settings > Face ID & Passcode (or Touch ID & Passcode on older iPhones), Enter your existing passcode, and then tap on Passcode Options to get a set of options.

Reduce Lockscreen Time To Minimum

The shorter you set the lock screen timeout setting (options are ranging from 30 seconds to never), the faster your iPhone or iPad display will require authentication to access it. You can change the auto-lock time by going to Settings > Display & Brightness > Auto-Lock.

Hide Notification Previews

Prevent random snoopers from seeing your data by hiding notification previews. Go to Settings > Notifications, then tap on Show Previews and choose When Unlocked.

Turn On Automatic Updates

Go to Settings > General > Software Update > Automatic Updates.

Don’t Reuse Passwords

If you use the iCloud Keychain to store web passwords, you can use it to check for password reuse. Go to Settings > Passwords & Accounts > Website & App Passwords. You will see a grey triangle with an exclamation mark next to any entry that is reused. To change the password, tap Change Password on the website.

6.2. Safer Software Updates and Practices.

Software updates include repairing security holes that have been discovered and fixing or removing computer bugs.

Advantages of Installing Software Updates.

- Software updates provide more than just security updates, they often offer new and improved features and speed enhancements to make the end-user experience better.
- Outdated and ineffective systems and software can hamper how people work with or for an organisation, causing frustration.
- Updates help patch security flaws.
- Hackers can take advantage of the weakness by writing code to target the vulnerability. The code is packaged into malware short for malicious software.
- When new software and upgrades are made available, existing systems and software may not always remain compatible, so it’s important to consult with an IT professional to ensure this process runs seamlessly.

Practical Demonstration 1: Turning on Automatic Updates in Windows 10 Devices.

1. Select the **Windows** icon in the bottom left of your screen.
2. Click on the **Settings Cog** icon.
3. Once in **Settings**, scroll down and click on **Update & Security.**
4. In the **Update & Security** window click **Check for Updates** if necessary. To check if your updates are paused, click **Advanced Options**. Some feature updates will need to be manually enabled even when automatic updates are turned on. To do this go to, Settings > Update & Security > Windows Update and select Check for updates. Once the update appears, you can select Download and install now.

Practical Demonstration 2: Enabling Automatic Updates on Android Devices.

1. Open Google Play Store.
2. Touch the hamburger icon in the top-left, swipe up and choose **Settings**.
3. Under General, tap **Auto-update apps**.
4. If you want updates over Wi-Fi only, choose the third option: **Auto-update apps over Wi-Fi only**.
5. If you want updates as and when they become available, choose the second option: **Auto-update apps at any time**.

Practical Demonstration 3: Enabling Automatic Updates on Apple Devices (iPhone)

1. Start the Settings app.
2. Tap "General."
3. Tap "Software Update."
4. Tap "Automatic Updates."
5. Turn on Automatic Updates by swiping the button to the right.

General Mobile Phone Safety Tips and Best Practices

1. Put a passcode on your phone.
2. Turn off location sharing.
3. Turn off Bluetooth when not using it.
4. Always check your privacy & security settings.
5. Always use anti-virus and anti-spyware software on your phones.
6. Do not store sensitive information on their phone.
7. Always review the applications you download.

Appendices

Appendix 1: Digital Security Resources for Structurally Silenced Women

Below is a collection of other useful digital security materials that you can use in addition to this training manual.

- **Guide to Secure Group Chat and Conferencing Tools**:

With people increasingly working remotely during COVID-19, we are all facing questions regarding the security of our communication with one another. Front Line Defenders presents this simple overview which may help you choose the right tool for your specific needs.

- **Umbrella**:

Umbrella is digital and physical security for people at risk on your Android phone. The Umbrella app brings together tools and advice on how to operate securely. Simple, practical advice from sending a secure email to secure travel.

- **Security in-a-Box**:

Security in-a-Box is a guide to digital security for activists and human rights defenders.

- **Access Now Digital Security Helpline**:

Offers direct, real-time, technical assistance and advice for activists, journalists, human rights defenders, and other members of civil society.

- **Digital Security & Privacy Manual**:

This book is an introduction to the ever growing and complex world of electronic security. Not only will it raise your level of knowledge and awareness about computers and the Internet, it will also warn you of different risks you may face in the digital environment and will tell you how to deal with them.

- **Digital First Aid Kit**:

This Kit offers a set of self-diagnostic tools for human rights defenders, bloggers, activists and journalists facing attacks themselves, as well as providing guidelines for digital first responders to assist a person under threat.

- **Surveillance Self-Defense**:

Surveillance Self-Defense is the Electronic Frontier Foundation's guide to defending yourself and your friends from surveillance by using secure technology and developing careful practices.

- **Information Security for Journalists**:

This handbook is a very important practical tool for female journalists and it is of particular importance to investigative reporters.

- **Totem Project**:

Totem is an online platform that helps journalists and activists use digital security and privacy tools and tactics more effectively in their work.

Appendix 2: References.

- Simplified Guide on Digital Security Best Practices. https://digitalhumanrightslab.org/resources/simplified-guide-on-digital-security-best-practices/
- Digital Security Training Curriculum.
  https://digitalhumanrightslab.org/resources/digital-security training-curriculum.
- Digital Safety Trainers Assistant. https://safesisters.net/wp-content/uploads/2019/09/Digital-Safety-Trainers-Assistant-smaller.pdf
- Modern Practice of Adult Learning. https://www.umsl.edu/~henschkej/articles/a_The_%20Modern_Practice_of_Adult_Education.pdf
- Level-Up Trainer's Curriculum. https://level-up.cc/curriculum/
- Security Education Companion: https://sec.eff.org/
- https://www.kaspersky.es/blog/digital-detox-advices/6226
- https://myshadow.org
- https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
- http://www.europe-v-facebook.org
- https://level-up.cc/curriculum/protecting-data/creating-and-managing-strong-passwords/input/safer-password-practices/

WOMEN AND ICTS

WOUGNET

WOMEN OF UGANDA NETWORK

Plot 360 Kiuliriza Kansanga - Gaba Road

P.O. Box 4411, Kampala (Uganda)

Tel: +256 394823109, +256 414532035

info@wougnet.org

@wougnet1

@wougnet

https://www.wougnet.org