Training Outline - Basics of Digital Security

Title: Digital Security Basics **Time:** 4 hours

Target audience: Members of grassroots organizations/small NGOs that are targeted online for their politically sensitive advocacy work

Aim
The aim of this training is to create a baseline of understanding of existing threats, as well as show tools and practices that can help protect organizations from the harm caused by online targeting.

Objectives
By the end of the session, participants will be able to:

- Identify what is a safe password to use for their online accounts
- Use a password manager to create and store passwords for their online accounts
- List at least 4 signs of a potential phishing email
- Identify the dangers of a ransomware attack
- List the steps to follow when suspecting an online attack

Methodologies and timings

Time	Trainer outline	Resources / Materials
In mins	Give an overview of each session with key content and intended methodologies. Indicate any breaks.	List materials needed
5	Icebreaker: Object near you (Will be useful for password generation)	
20 + 10	Goal: Explain the two characteristics of a good password: uniqueness and length. Practice: Audience will then be asked to determine which passwords are good from a list drawn from a hat. Breakout rooms: come up with as many passwords that fit the above criteria as possible. Do not write them down. 10 min	- List of top 1000 used passwords - Jamboard to create as many passwords that fit the two criteria above as possible.

30 + 10	Open-ended question: how many passwords you've created have you been able to remember? Did any one use objects near them to create passwords? Goal: introduce password manager Video: how to use a password manager Break: 10 min	- Statistic: Find average number of online accounts each person has nowadays - Setup for presenting video
15 + 10 + 10 + 15	What is a phishing email? What are the usual signs of a phishing email? How is it different from a spam email? What is the purpose of a phishing email? Video: correspondence with scammer Breakout rooms: Open your email inbox right now, and share share examples of phishing emails you've received in the past. Recommend checking the spam folder. Once you find one example, send it to this address <> Presentation: show examples on screen. Try to identify as many signs of a phishing email as possible Signs are: sense of urgency, unusual request, grammar mistakes, unfamiliar greeting, unrecognized contact	- Setup for presenting TedTalk video - Backup examples of phishing emails