**Exercise 5: Backup Fest**

**Intro:** Hands-on exercise to teach participants how to back up, reformat, and restore data to their phones.

**Timing:** 1.5 hours

**Equipment Needed:**

* Whiteboard or paper and markers to outline instruction content, participant’s contributions, and take notes.
* Mobile phones.
* Computers (ideally participants’ own; if not suggest they bring memory sticks).
* Participants should be asked to bring the data cables for their mobile phones, and any software that came with the phone e.g. Nokia PC Suite, iTunes.
* Trainers should have their own copy of any backup software they are able to download.
* Internet access in the training venue (optional but helpful).

**Content Outline and Main Topics:**

1. **Discussion (10-15 minutes)**: How vulnerable is your physical device?
2. **Discussion (10-15 minutes)**: What is a secure location?
3. **Exercise/Instruction (45 minutes)**: Backup Fest.
4. **Discussion (10 - 15 minutes)**: What’s your backup plan?

**Objectives/Expected Outcomes:**

* Participants will learn how to protect their data by backing it up, wiping it from their phone, and restoring it.
* As desired, this session will also cover encrypted storage for backups on a PC.

**Additional Resources for Trainers and Participants:**

Backups, Data Deletion and Remote Wipe Tools //LINK//

[Nokia Synchronizing and Copying FAQ](http://www.nokia.co.uk/support/faq/synchronising-and-copying)

[iPhone and iPod Touch Backups using iTunes](http://support.apple.com/kb/ht1766)

[Security-in-a-box chapter on encryption using TrueCrypt](https://security.ngoinabox.org/chapter_4_1)

[Protektor manuals](http://protektor-blog.blogspot.com/)

**Content**

**1. Discussion (10-15 minutes)**: How vulnerable is your physical device?

Begin this section by discussing the vulnerabilities of devices and the importance of data.

Questions to ask:

* Who has ever lost a phone, had a phone taken from them, or dropped a phone in water?
* Who has ever had a phone that stopped working? Did you lose your data?

The safest way to protect data on your phone is not to have data on your phone in the first place! For situations where you face the threat of seizure or loss of your device, consider:

* Using a different device that you keep “clean.”
* Removing the data from your phone and storing it in a secure location.

Your phone may break or stop working for some other reason. Always protect your information by backing it up to a secure location

**2. Discussion (10-15 minutes)**: What is a secure location?

This depends on your situation.

Questions to ask:

* Where do you store your most sensitive information?
* What measures do you already take to protect sensitive information?

Things to highlight:

* In this case, find and choose a storage device that is more secure than your mobile.
  + One that is less likely to be seized, lost, or damaged.
  + One that if seized, lost, or damaged, will be less obvious that the data is on it or the data will be more difficult to access.
  + One that protects your backups as much (or more, if it’s more sensitive) as your other sensitive information.

Questions to ask:

* Secure locations on your computers or physical storage? How vulnerable are your computers and hard drives?
* Secure locations in the cloud? How well protected is cloud storage?
  + Your cloud storage provider can usually access your data, for example, they may do this in response to requests from law enforcement. Do they have an explicit policy on this, and are you comfortable with their track record? [The EFF keeps a ‘report card’ on privacy policies](https://www.eff.org/pages/when-government-comes-knocking-who-has-your-back).
  + Have you read the terms of use for your cloud storage provider, and your other online services? Check <https://www.eff.org/issues/terms-of-abuse> for why this is important.
  + Do you trust the security provisions of your cloud storage provider?
  + As further reading, here’s a [dated but useful discussion of what cloud storage is, and the security implications](http://www.pbs.org/newshour/bb/science/july-dec09/cloudcomputing_07-09.html).
* Password protecting and encrypting data:
  + Set good passwords. Remember, good passwords are:
    - Not a single dictionary word. Consider using a short phrase.
    - Not easily guessed by someone with access to your personal details. For example, don’t use your name, the name of a family member, your birth date, address, or hometown.
    - Ideally, contains letters and numbers.
    - Not re-used for other accounts on different websites.
  + Encrypt your backups, but beware the limitations of encryption (for more see <https://security.ngoinabox.org/en/chapter-4>).
    - If you lose your password or encryption key, your backup is useless (with cloud providers, they can usually get the data back for you).
    - The presence of encrypted data on a file system can draw attention to your sensitive data.
    - In some countries, encryption is illegal and/or you may be forced to reveal your password.

**3. Exercise/Instruction (45 minutes)**: Backup Fest.

Walk participants through the backup process: Choosing a backup plan, backing up to an online service or to an SD card, copying data to a computer, encrypting data on that computer, reformatting a mobile, and restoring the data.

Have participants group by OS/handset and gather around a computer, one group at a time. Work with participants to understand the backup methods they choose, understand what will and won’t be backed up (apps, contacts, call logs, or sent messages), and then to perform the backup. You may include some or all of these steps:

* Creating a backup. See Backup, Data Deletion and Remote Wipe tools //LINKS// for options for different phones, as well as the phone manual. For a phone with a memory card, also back up the contents of the memory card to a PC.
* Erasing all data from the phone. (See [Recellular Data Eraser](http://www.recellular.com/recycling/data_eraser/) for information about how to do this. BE WARNED! This is only for phones you are sure have been backed up.)
* Restoring the data using the backup app.
* Installing [SaferMobile InTheClear](http://safermobile.org/wiki/InTheClear) or another remote wipe app from Backup, Data Deletion and Remote Wipe tools
* If desired, include [encryption using TrueCrypt](http://www.google.com/url?q=https%3A%2F%2Fsecurity.ngoinabox.org%2Fchapter_4_1&sa=D&sntz=1&usg=AFQjCNEU8JCuvnuVKCna5MqfnFdgpu_W5w) for backups made to a PC.

**4. Discussion (10 - 15 minutes)**: What’s your backup plan?

Ask participants how often they think they need to back up their data. Should they keep extra copies of their backups, in case multiple devices are stolen or seized? Emphasize the importance of having a backup policy (and a larger security policy) as opposed to doing one-off backups or only in response to particular incidents.