Encrypt data using 7-zip

Keep Research Data Securely
Data Encryption
Beginner

Introduction

This document outlines how users can use 7-zip to create an encrypted zip file to protect data.

Further information on data encryption may be found on the LSHTM Research Data Management pages hosted on Sharepoint:

https://lshtm.sharepoint.com/sites/intranet-library-archive-and-open-research-services/SitePages/Research-Data-Management.aspx

What is Encryption?

Encryption is a process through which data – digital or otherwise – is encoded in a form that makes it difficult to read by a non-authorised third party. It may be compared to a process of protecting a physical object by placing it in a box and locking it. In order to access the objects, the data holder must possess a key capable of unlocking the box. Encryption is commonly used by researchers to protect confidential and sensitive data.

Compression software

A number of compression tools support password protection and encryption, including Winzip, 7-zip, p-zip, and others. These software tools can be obtained from the relevant website or via the app marketplace for your operating system.

For this tutorial, we will be using 7-Zip, an open source file archiver that is available for Microsoft Windows, Apple Mac OS, Linux, and other platforms. This can be downloaded at http://www.7-zip.org/.

Install the compression tool

7-zip must be installed on your computer prior to use. The installer will prompt you to make decisions on the preferred installation folder, file associations, and other configuration settings

Library, Archive & Open Research Services
https://www.lshtm.ac.uk/research/library-archive-open-research-services
library@lshtm.ac.uk
+44 (0)20 7927 2276

LONDON SCHOOL of HYGIENE &TROPICAL MEDICINE

Create an encrypted archive containing multiple files

The simplest way to create an zip file is to copy the files that you wish to include into a folder and compress the folder. This may be achieved as follows:

a. Right-click on the folder to be compressed.

b. Select the “Add to archive...” option from the menu. *DO NOT* choose the “Add to FILENAME.zip option – this will create a compressed archive, but will not provide you the option to password protect or encrypt the archive.

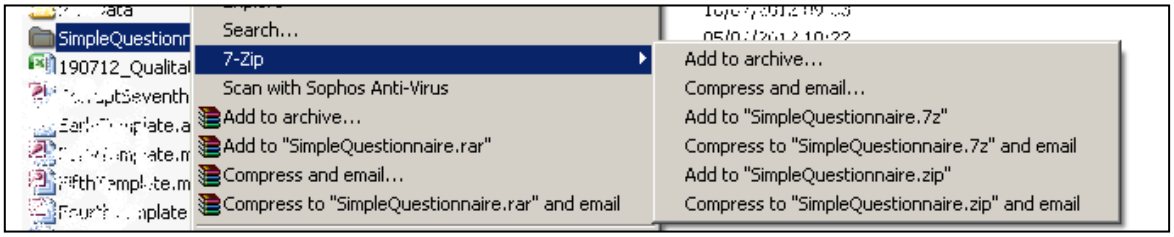

Figure 1: 7-Zip compress menu options

c. A dialog box will appear, as shown in Figure 2.

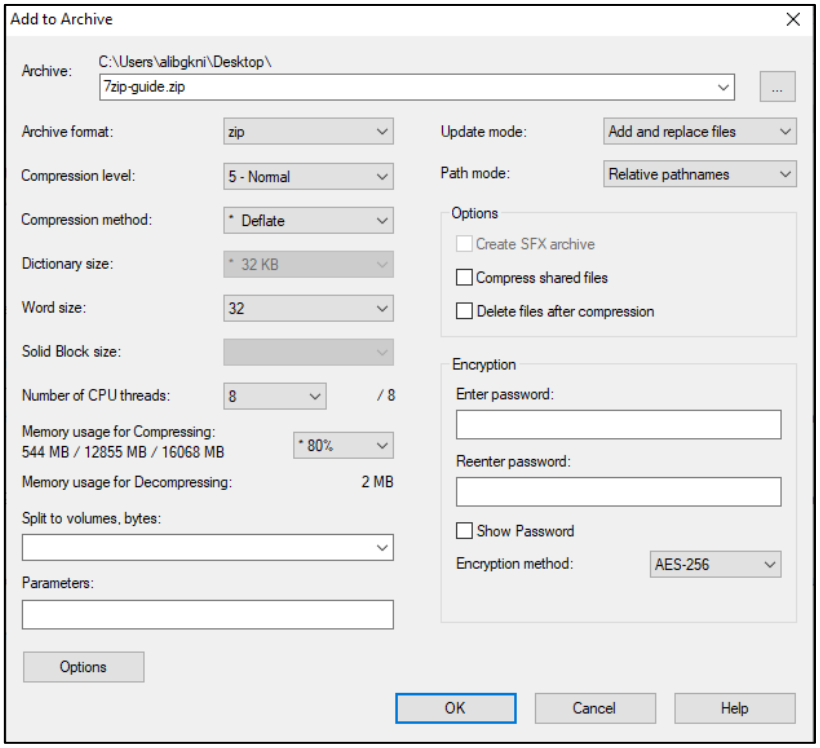

Figure 2: Archive configuration options

d. Choose an archive format to use. ZIP is suitable for most purposes.

e. Choose a strong password and type it into the Encryption section. The password should ideally be 10+ characters and consist of letters, numbers and special characters. Upper and lowercase letters should be used.

f. Set the Encryption method to AES-256 and click OK.

If the compression process has completed, but you cannot see the zip file, refresh the window by pressing F5 on the keyboard.

1. Test the archive encryption

To ensure the compressed archive has been encrypted, it is advisable to test it before sending it to others. This may be achieved by performing one of the following steps:

a. Right click on the compressed file, navigate to the 7-Zip sub-menu, and select the “Extra to “Foldername\” option.

OR

b. Right click on the compressed file, navigate to the 7-Zip sub-menu, and select “Open Archive” option to display the contained files in 7-Zip.

c. Press the Extract button and choose a suitable folder to extract the files. This *MUST NOT* be the same location as the original files - it will attempt to overwrite them.

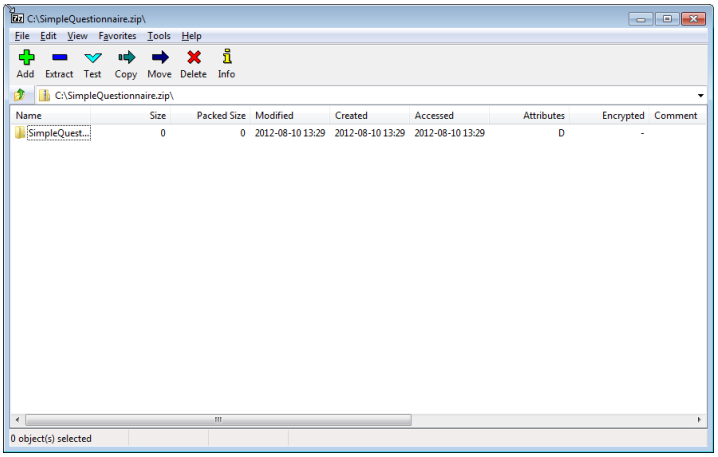

Figure 3: Compressed archive shown in a 7-Zip window

d. If the encryption has been applied successfully, you should be asked to enter a password. Enter the password and press the OK button.

- If the correct password has been entered, the files held in the archive will be written to the chosen destination folder.

- If an incorrect password has been entered, an error message will be displayed indicating an extraction error. Files may appear in the destination folder, but they will be zero kilobytes in size - no content will be extracted.

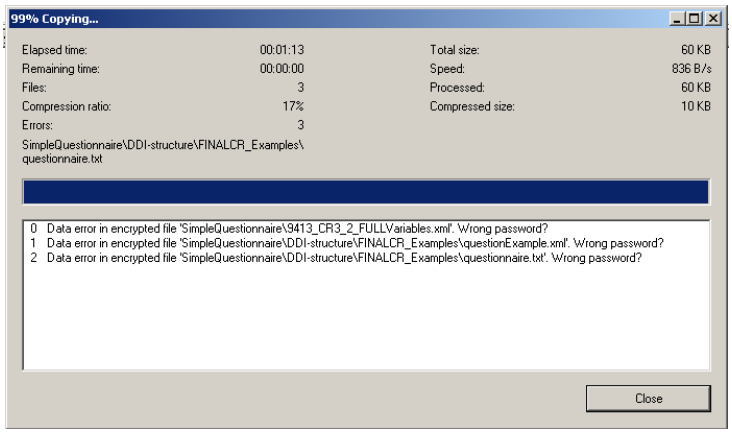

Figure 4: Data extraction error message

2. Send encrypted archive to the intended recipient

The final step is to send the encrypted archive to the intended recipient and provide them with the password separately.

a. LSHTM provides several platforms for sharing files with internal and external collaborators, including Zendto, Onedrive, and MyFiles. The chosen platform should be appropriate to the Classification level, as outlined in the LSHTM Data Classification and Handling Policy.

b. The password may be communicated with the intended recipient(s) via telephone, instant messaging, email, or other methods (such as https://privnote.com). To minimise risk of interception, the password **MUST NOT** be sent with the archive itself.

How do I get more help?

The LSHTM Open Research team provide advice and guidance on topics related to the creation, management, and sharing of research data. Information material and contact details are available on the LSHTM Research Data Management pages on Sharepoint. https://lshtm.sharepoint.com/sites/intranet-library-archive-and-open-research-services/SitePages/Research-Data-Management.aspx