

Encrypting and Sending Files

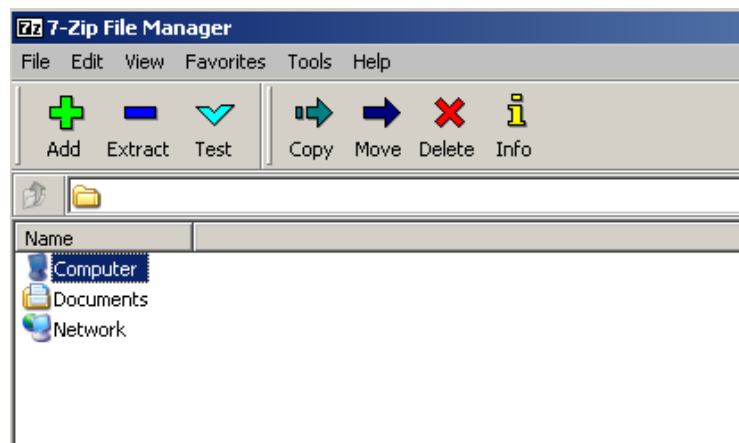
Encrypting files prevents them from being accessed by anyone without the password.

Note: If you lose the password the file CANNOT be recovered under ANY circumstances.

The process below uses a program that is deployed onto all University corporate desktops and is also available for free from: <https://www.7-zip.org/>. This document should always be read in conjunction with the University Acceptable Use Policy when handling personal or sensitive data.

Encryption Procedure

When installed, the 7-Zip program can be found through the Start Menu. You should be able to find it in your Accessories (Windows Accessories on Windows 10) folder under 7-Zip. Open 7-Zip File Manager.

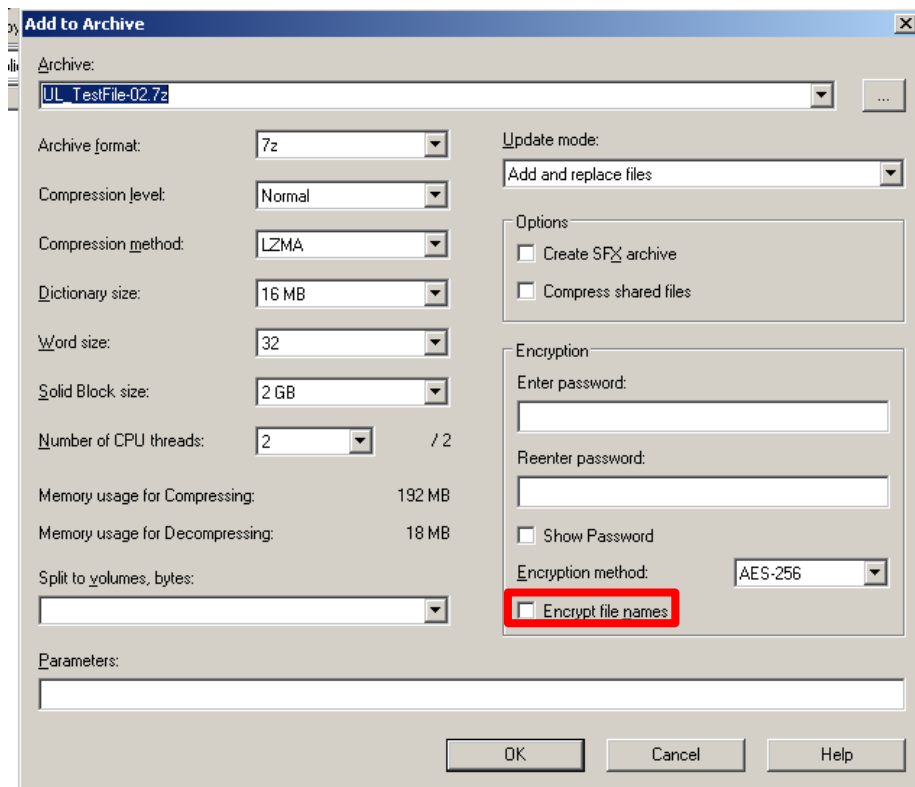


This opens the 7-Zip console window as shown in the image above*.

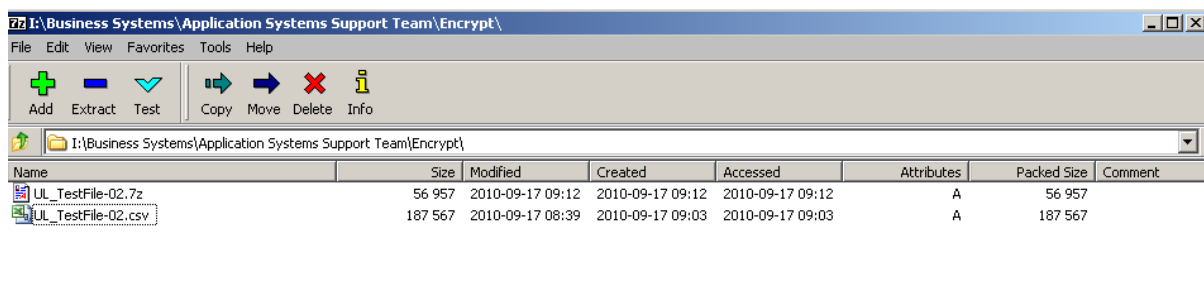
**Please note the first time used shows the window as Fig. 1 subsequent runs keep the last path navigated to.*

1. Navigate to the folder and file(s) to be encrypted in the way you would normally find files on your computer. Please note that there is a delay after clicking the Computer name before all your drives are shown.

- Highlight the file(s) you wish to encrypt and click the 'Add' icon. This will cause the next window to be shown (see below).



- In the section labelled 'Encryption' in the bottom right of the window, enter a custom password and the re-enter password for confirmation.
- Ensure 'Encryption method' is AES-256 (This is a drop-down menu but there is only one option.)
- While adding files to 7-zip archive, just below the passwords field there is an option to encrypt the file name. Select the Encrypt file names option (see red highlight)
- Click OK and the 7-zip console window reappears as below.



As shown above, the encrypted zipped file is in the same path as the original file with a .7z file extension.

Giving the Recipient the Encryption Password

To extract and decrypt the files, the recipient must use the password that was used to encrypt them.

However, the password must be given to recipient by a different method than the file. For example, if the file is emailed the password can be given by phone or text.

This is to prevent anyone intercepting the encrypted file from intercepting the password at the same time.

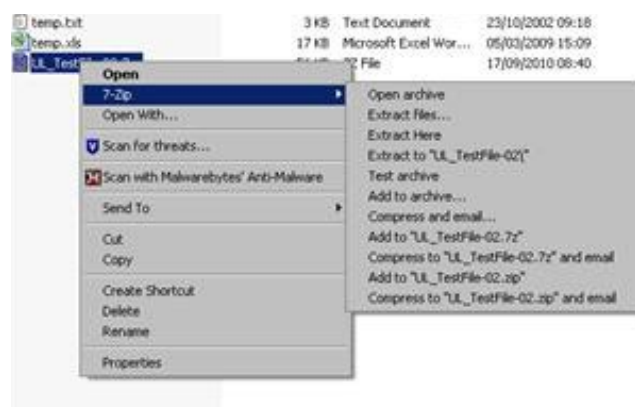
Receiving Encrypted Files

To access files that have been encrypted using 7-Zip you must have 7-Zip installed. It can be obtained from: <https://www.7-zip.org/>. If it is not possible for the recipient to install 7-Zip, then this software cannot be used to securely transfer information.

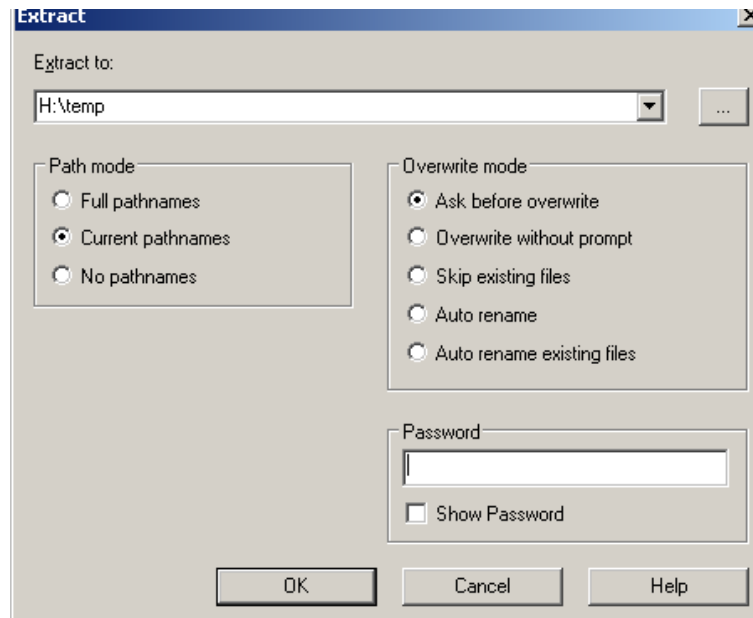
If the recipient is not able to install 7-Zip, ask them how they can receive files securely. They may have a secure web site or use another secure method. Please ask ICT for help if needed by calling 01522 88 6500 or emailing ict@lincoln.ac.uk.

Using 7-Zip to Receive Encrypted Files

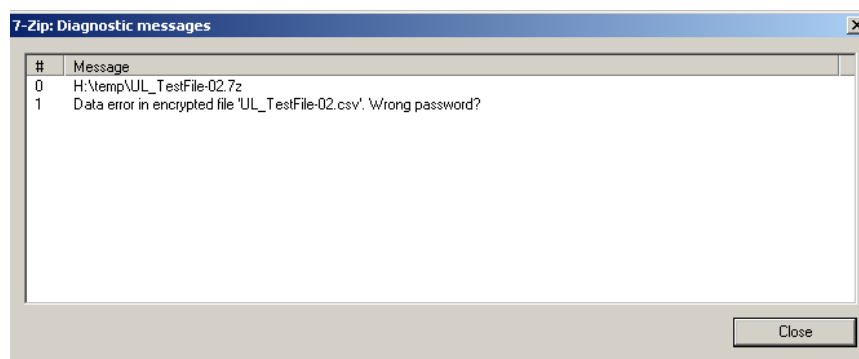
1. Save the encrypted zipped file attachment to a folder.
2. Right-click on the file and the 7-zip menu appears (see below).



3. Select 'Extract files' and the window below will appear:



4. Change the 'Extract to:' drop-down folder as required.
5. Enter the password supplied by the file sender into the 'Password' box (this password should have been sent through separate means to the file itself).
6. Click 'OK'.
7. If the password is correct the file(s) are extracted and can be used as normal.
8. If the password is incorrect the window below will be shown. Please note the folder & file will be created with the file being empty.



9. Try the extract again and if the password is still not accepted contact the sender for confirmation.