



The Last Messages Club

Special Encryption Techniques

Contents:

- Section 1: introduction
- Section 2: encryption with WinZip®
- Section 3: encryption with Axcrypt®
- Section 4: Passwords

Section 1: Introduction

The Last Messages Club recommends that any especially sensitive information is encrypted using one of the popular, easily available but reliable encryption techniques. To do this you would create your documents, videos, pictures or sound files in the normal way and then encrypt the files. Finally you would attach the encrypted files to one or more of your Last Messages.

Your recipients will be able to read your Last Messages and therefore your instructions for opening the attachments.

Encryptions rely on passwords and the fourth section of the document outlines some useful ideas about the selection and use of passwords.

Below we explain how to encrypt files with two popular tools.

We also provide some guidance on creating safe passwords.

Section2: Encryption with WinZip®

This section explains how to encrypt attachments to Last messages using the WinZip® toolset.

1: If you do not already own a copy, purchase and install a full version of WinZip® (the version that forms part of Windows does not offer proper encryption).

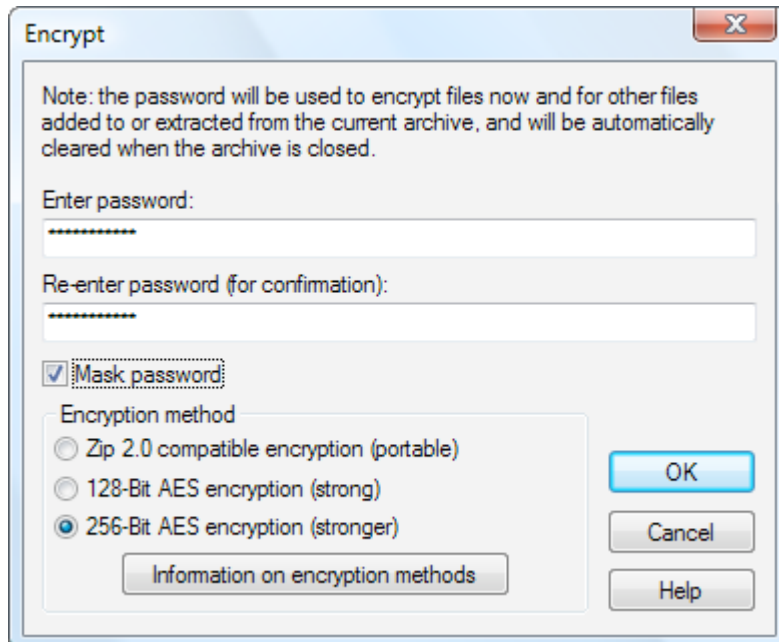
<http://www.WinZip®.com/index.htm>

2: Create a new archive using the 'New' button and give the archive a suitable name

3: Add the files you wish to encrypt to the new archive making sure you click on the 'encrypted' radio button

4: You will be asked to enter a password twice. We recommend using a two part password in this form: firstpart-secondpart.

5: Save the encrypted archive and attach it to a last message as an attachment



6: Include the first part of the password in the relevant last message accompanying the attachment and send the second part to one or more of your Trusted Advisers explaining your encryption process and password method.

You must provide your intended recipient with the information needed to open the attachment including the complete form of the password, the first part of the password and the trusted adviser(s) contact details.

Only your intended recipient will be able to open the attachment by collecting the message, collecting the second part of the password from a Trusted Adviser and assembling the password.

If your intended recipient is one of your trusted advisers you can give part of the password to another trusted adviser.

Here is some suggested explanatory text for the Last Message that accompanies the encrypted attachment:

For reasons of security I have password protected the attached file. You should be able to open the attachment by double clicking on the attachment icon but you will be asked for a password.

*The password you will need is in two parts separated by a hyphen
e.g. firstpart-secondpart*

The firstpart of the password is: xxxxxxxx

*These people have the second part of the password:
Name and contact details of trusted advisor(s)*

*WinZip® is a Registered Trademark of WinZip® International LLC
WinZip® 's advanced encryption (FIPS-197 certified) uses the Rijndael cryptographic algorithm which, in 2001, was specified by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standards (FIPS) Publication 197 as the Advanced Encryption Standard (AES). After a three-year competition, the AES was announced by NIST as an approved encryption technique for use by the U.S. government, private businesses, and individuals. When properly implemented as a key component of an overall security protocol, the AES permits a very high degree of cryptographic security, yet is fast and efficient in operation.

Section 3: Encryption with Axcrypt®

This section explains how to encrypt files using the Axcrypt software tool.

1: If you do not already own a copy, download and install a full version of Axcrypt®.

<http://www.axantum.com/AxCrypt/>

Axcrypt is produced by Axantum Software AB

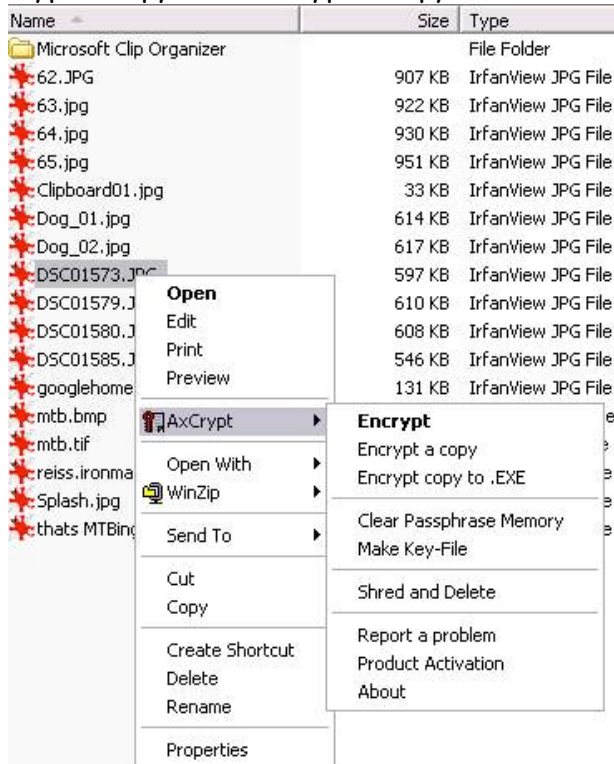
Axcrypt® claims to offer a much safer encryption than other popular encryption tools and is free of charge.

2: Select the first file you wish to encrypt in Windows Explorer

3: Right click and select Encrypt

Note: 'Encrypt' causes the original file to be deleted.

'Encrypt a copy' and 'Encrypt a copy to EXE' both leave the original file intact.



4: The Axcrypt® dialog will appear requesting you enter a password twice (known as a passphrase in this case). Leave the two check boxes unchecked as shown.



5: Axcrypt will create a new file for you using the suffix. .axx

6: Upload the encrypted file to your Personal Vault files collection and add it as an attachment to any messages as desired.

7: You must provide your intended recipient with the information needed to open the attachment.

You could include in your last message this explanation:

For reasons of security I have password protected the attached file. You should be able to open the attachment by double clicking on the attachment icon but you will be asked for a password.

*The password you will need is in two parts separated by a hyphen
e.g. firstpart-secondpart*

The firstpart of the password is: xxxxxxxx

*These people have the second part of the password:
Name and contact details of trusted advisor(s)*

Section 4: Passwords

Both you and your advisors should protect your files and data through the use of a suitable password. Regaining a lost password at the Last Messages Club website is a deliberately designed process to maintain your security.

New members and advisors are issued a temporary password and must change this to something more complex and memorable. Temporary passwords are always three lower case letters followed by three numbers.

You might visit <http://www.passwordmeter.com> for password design advice.

Password Protection for Special Encrypted Files

Special Encryption is ideal for very sensitive documents. You use one of the popular encryption software tools (WinZip®, Axcrypt® or others) to encrypt a document before attaching the encrypted file to a Last Message. This will be in addition to our normal encryption employed by the Last Messages Club for messages and attachments.

One possibility is to use a password that your recipient would recognise from a description or clue.

In the accompanying Last Message you might say:

The attached file is encrypted and you will need a password to open it. The password is your mother's maiden name/ Your first dog's name/ the nickname we used for your car.

Alternatively you might split your passwords by sending one half to your intended recipients and the other half to one or more of your Advisors. Your recipient will one day request the second half of the password from the Advisor and therefore be able to assemble the password and open the encrypted data.

You might consider protecting your double encrypted files using a two part password in this form: firstpart-secondpart. The hyphen clarifies the separation between the two parts.

You would then include the first part of the password in the Last Message accompanying the attachment and send the second part to one or more of your Advisors explaining your encryption process and password method.

The Last Messages Club and your Advisors will have no access to the whole key so will be unable to access your encrypted attachment or reveal it to anyone else. Only the recipient will get the whole key and be able to view the contents of the encrypted files.

You must provide your intended recipients with the information needed to open the attachment(s) including the complete form of the password, the first part of the password and the advisor(s) contact details.

Note: if your intended recipient is one of your advisors you can give part of the password to another advisor.