IPA Data Security:
Boxcryptor Basics with exercise

researchsupport@poverty-action.org

Learning objectives

- Understand why Boxcryptor is IPA's recommended encryption software

- Be able to implement basic encryption tasks such as encrypting a folder, and sharing an encrypted folder with additional users

Setting yourself up with Boxcryptor

- **Download & install Boxcryptor:** [Download](#) Boxcryptor for Windows or Mac.

- **For IPA staff, log in:** When you were hired, your manager should have opted to link a *paid* Boxcryptor institutional account to your IPA email. Check your email for an invite, or check the status of your account with the IT team by emailing support@poverty-action.org. *Never* create your own free account.

- **For non-IPA staff, create an account**: You can [create](#) your own free account online, or follow your organization's instructions.

J-PAL
ABDUL LATIF JAMEEL POVERTY ACTION LAB

Why does IPA use Boxcryptor for file encryption?

- It is the **type of encryption software required by IRBs** to ensure only the right people from your project can view sensitive data linked to PII (the type of "encryption" mentioned by services like Box and Dropbox, even if they areHIPAA compliant, is NOT sufficient for IRBs)

- It **works with both Box and Dropbox** (VeraCrypt does not work with Box)

- It **allows you to collaborate** and work with files easily (VeraCrypt can create conflicted versions of "container" files without careful management)

- It allows users to **manage their own passwords**

- It allows users to **grant granular, folder/file level access to other users**

- It offers **an institutional license** which provides IPA with additional opportunities to manage IPA users and files

J-PAL
ABDUL LATIF JAMEEL POVERTY ACTION LAB

A clarifying note on sharing settings

Boxcryptor sharing settings are *completely separate from Box or Dropbox sharing settings*

- For example, imagine that your "Project Folder" on Box is shared with a Country Director, three researchers, and eight other IPA colleagues.

- You use Boxcryptor to encrypt a subfolder on Box called "Baseline Data", and save the raw survey data there – great! But now no one can else see the data!

- You will need to use Boxcryptor to give *only those included on your IRB* permission to decrypt and view the data in the "Baseline Data" folder. Maybe that means three PIs and just two IPA colleagues. Once you share the folder through Boxcryptor with those five people, they will be able to decrypt and view the data. The remaining CD and six other colleagues will remain on the entire Box folder, but simply won't be able to decrypt/view the baseline data at all.
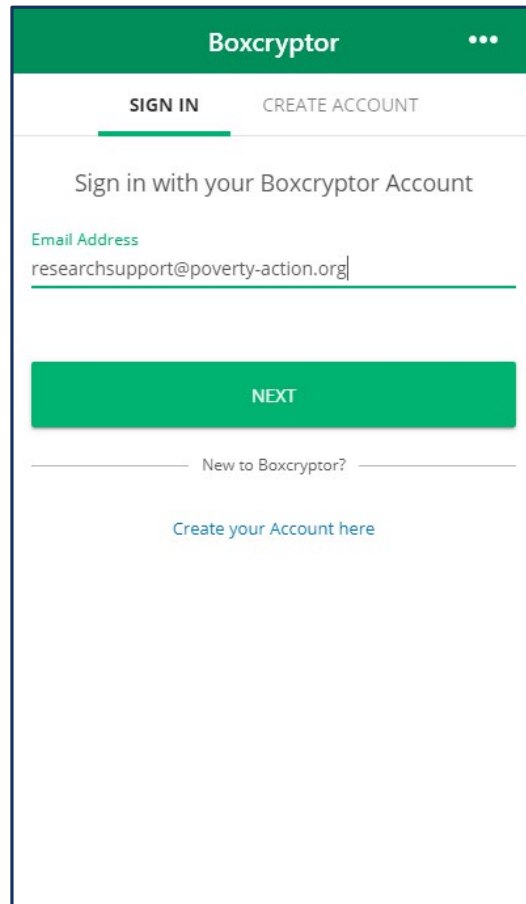
J-PAL
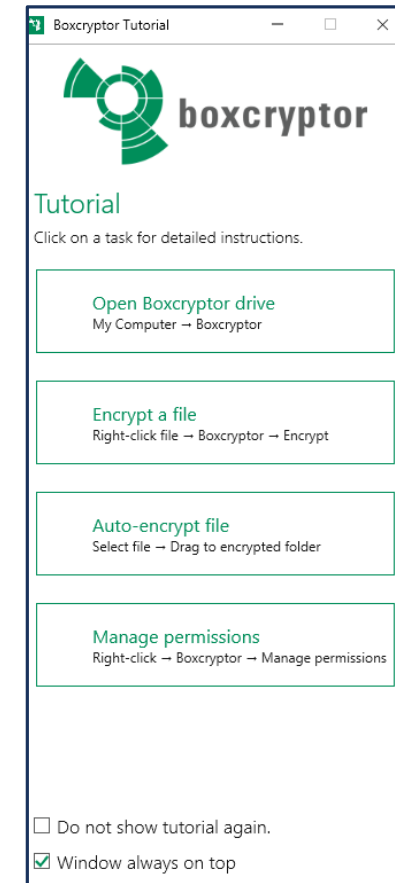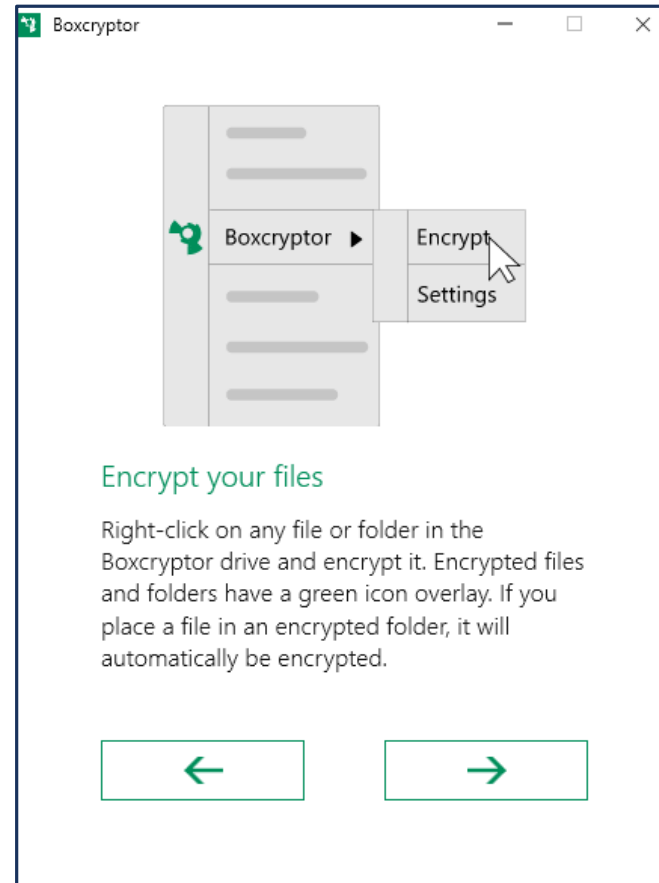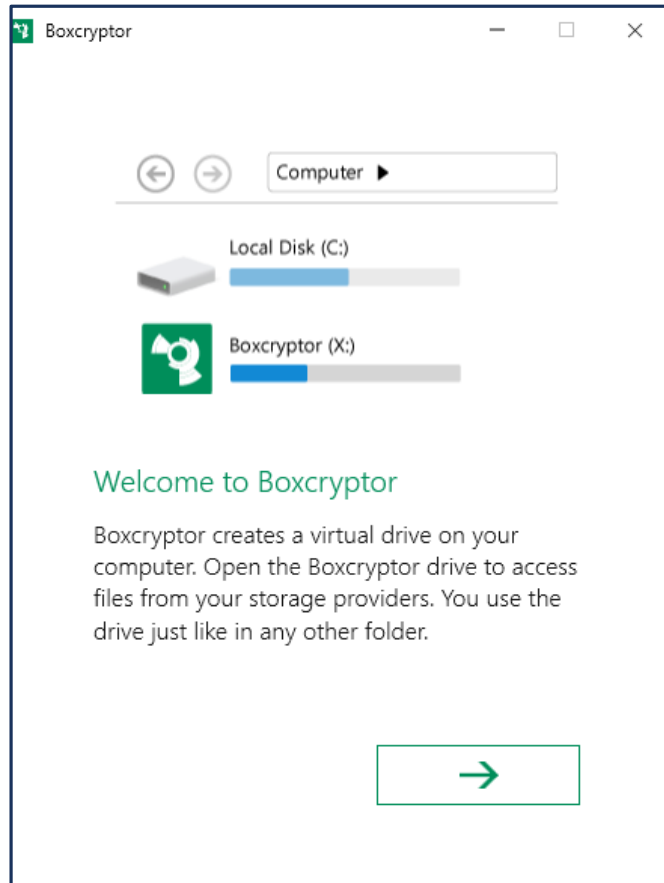ABDUL LATIF JAMEEL POVERTY ACTION LAB

Let's practice using Boxcryptor

Open Boxcryptor, and log in
Remember, you should already have either an IPA institutional account, or your own free account if you are not IPA staff
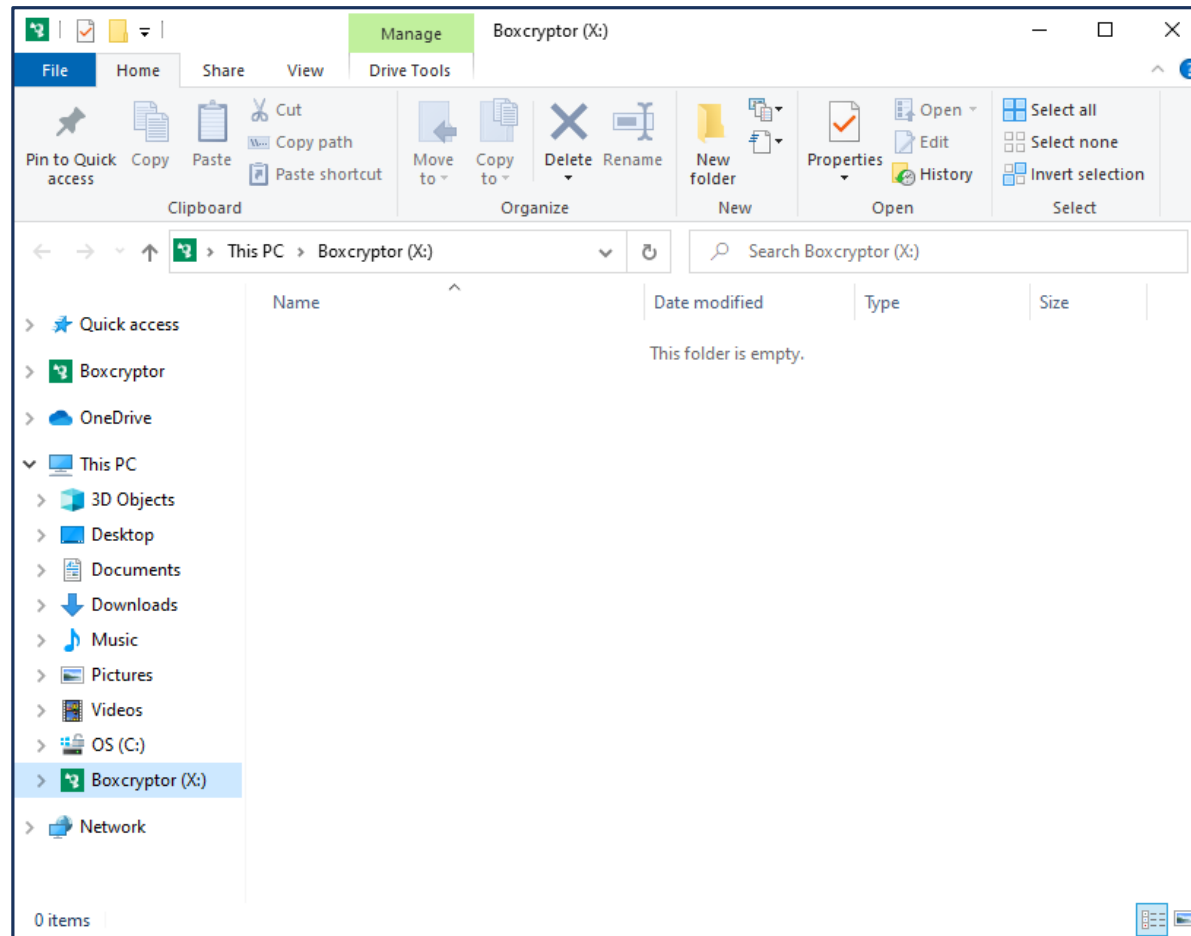
Click through the mini-tutorial

If this is your first time using Boxcryptor, take a few moments here – the short tutorial is very helpful!

Observe the X: drive

Your computer now has a mysterious "Boxcryptor (X:)" drive...

Create a test folder right on your desktop

You are NOT going to play around anywhere near your project data, please!!! First, create a folder on your desktop called "Demo" or "Test". Put a couple simple files inside, like Word or Excel documents. (You can try it out with Stata files later!) Just create a harmless folder and files for testing.
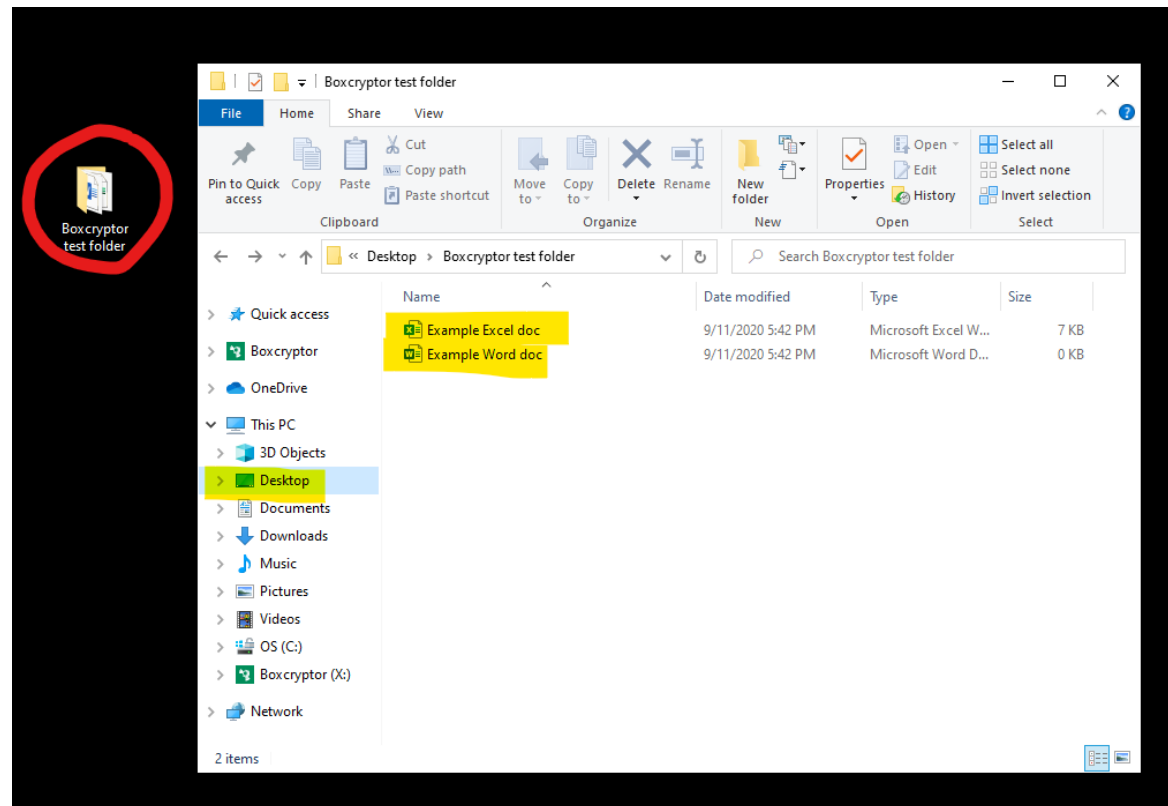
Add a "location" to Boxcryptor

Right click Boxcryptor (likely hanging out in your system tray) > Settings > Locations tab > Add button > Choose "Desktop" > Select Folder > OK.
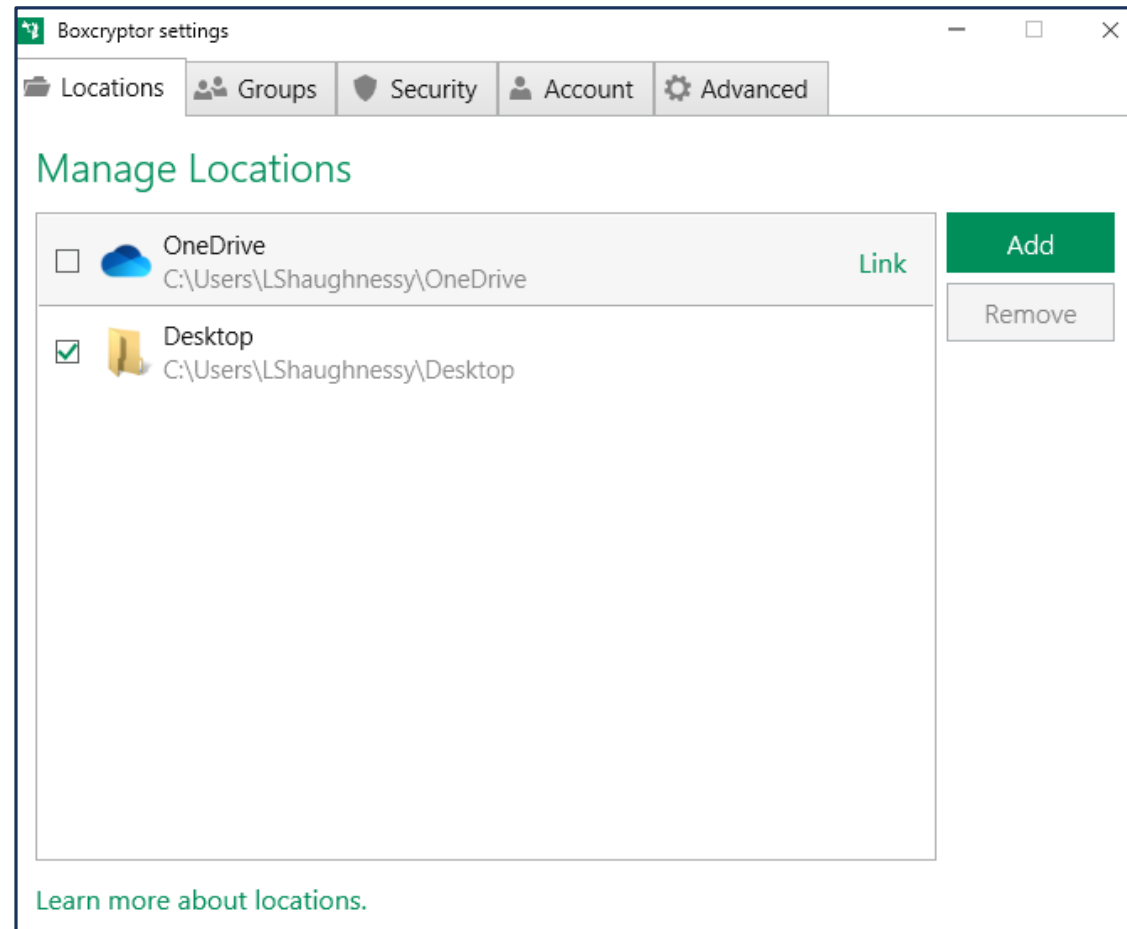
Tip: You can also add more useful locations like Dropbox or Box Sync.

Now go back to the X: drive

Observe that the X: drive no longer appears empty. Your Desktop is visible in X:, and you can open, view, and edit files from your "test" folder just like you would on your actual desktop. Try making edits through X: and then opening on desktop!
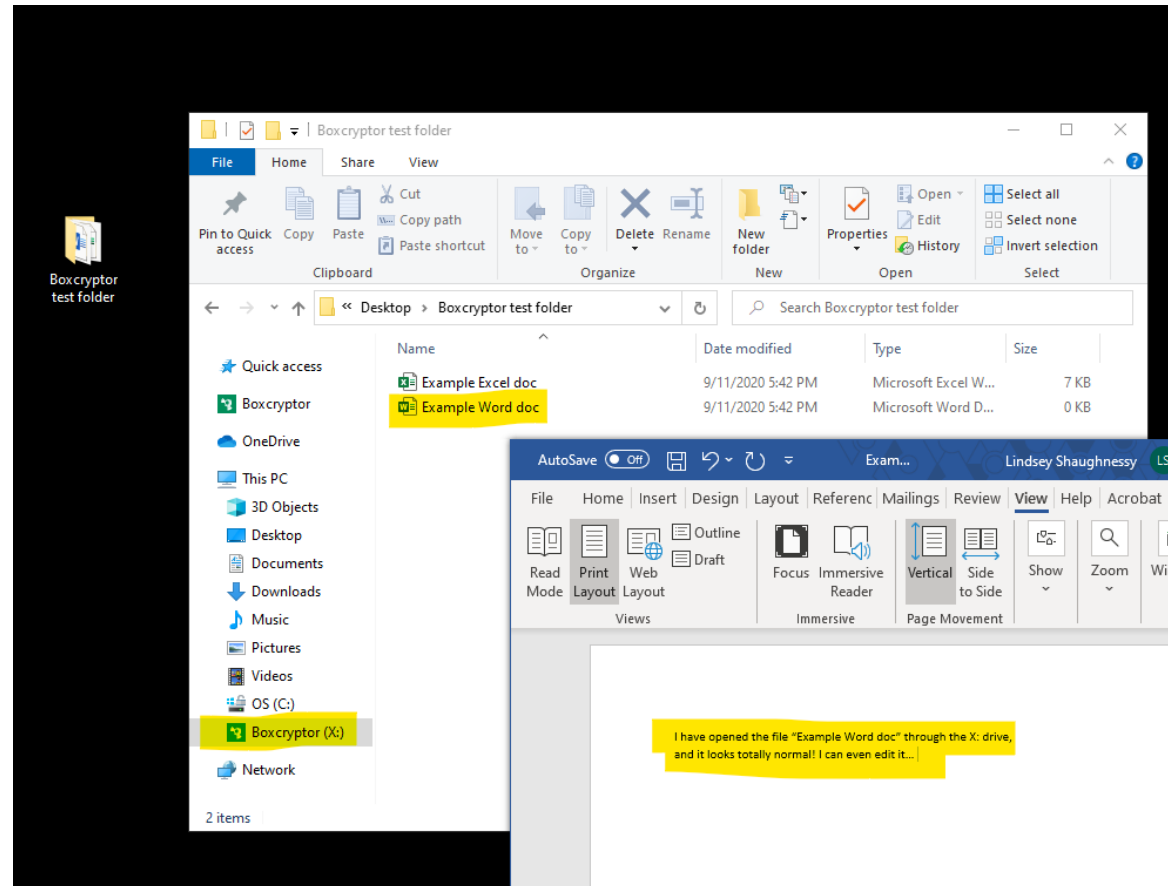
It's time to create an encrypted folder!

Make sure you are using the X: drive. Right click inside your test folder, select New > Folder. Boxcryptor will ask whether the new folder should be encrypted. Click "Encrypt" to create an encrypted folder! Name it anything you'd like, such as "My encrypted folder" or "Raw baseline data".
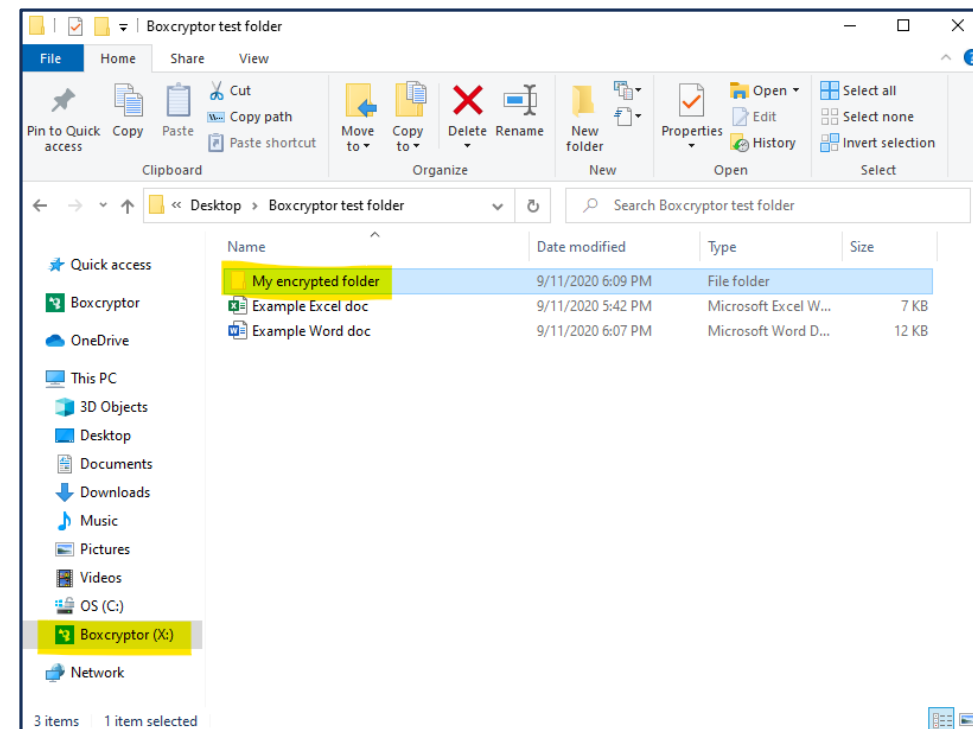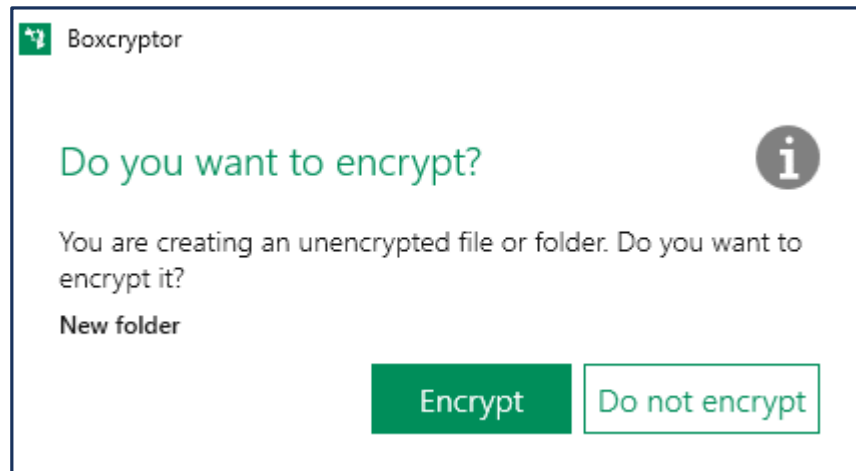
Add a file to your encrypted folder

You know the drill. This IS a test. Just add a Word document or Excel document or anything you'd like to your encrypted folder – but make sure you are using the X: drive. You can open, edit, view, save the file like normal.
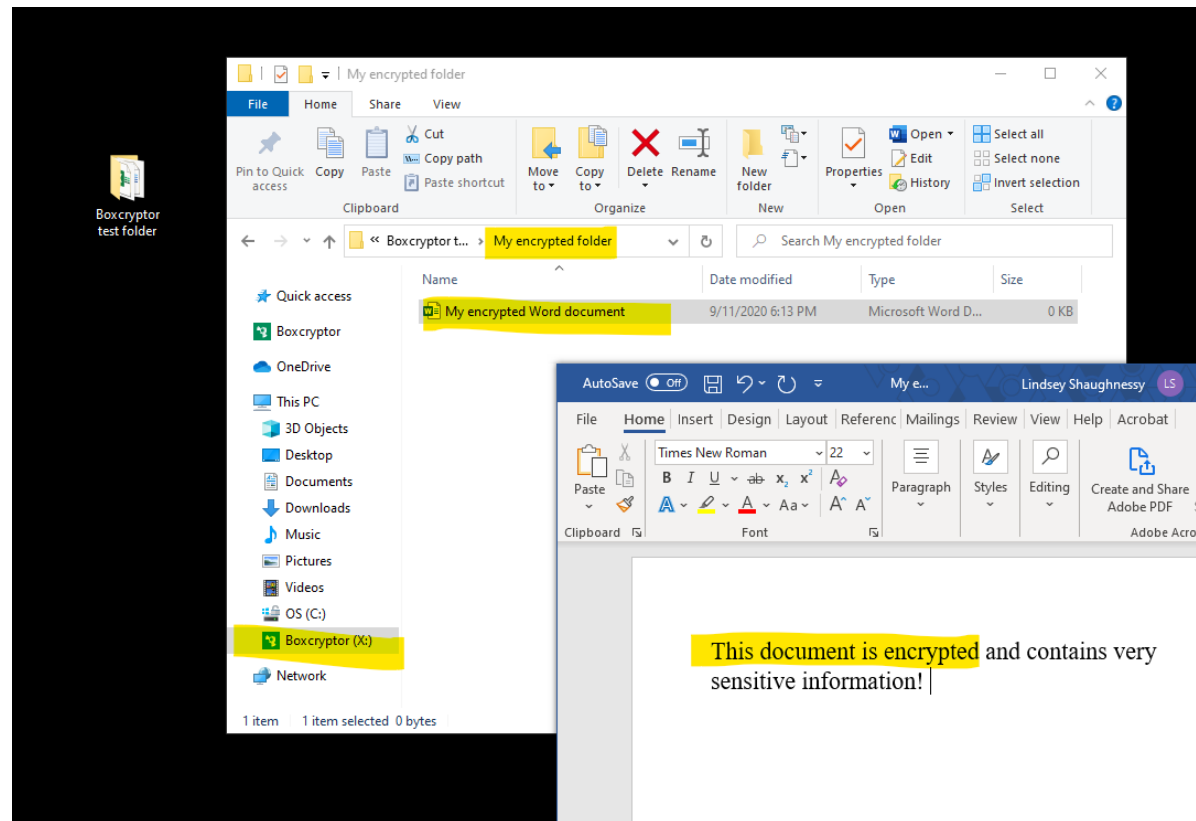
Now try to open that file through actual Desktop…

LOG OUT OF BOXCRYPTOR FIRST! Now try to open that same file in the encrypted folder through your desktop, NOT through the X: Drive. It's not possible. It's encrypted. It's as if you are not a user permitted to decrypt that file – it's because you are not accessing it through Boxcryptor.

Share an encrypted file

It's not very useful to have data only you can access. Log in to Boxcryptor. Get back on X:. Right click your *file*, select Boxcryptor > Manage permissions > Add user > enter "researchsupport@poverty-action.org" > OK > Apply.
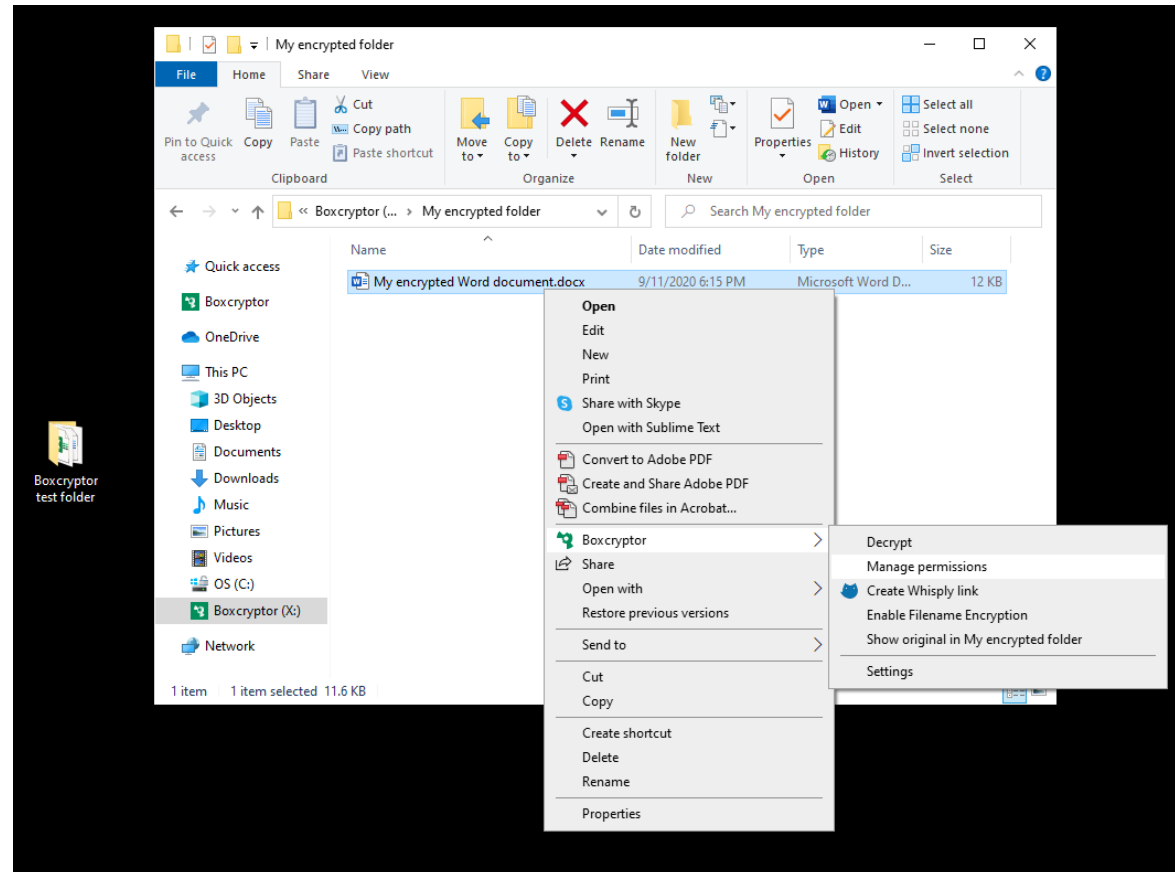
Send your encrypted file to IPA!

For IPA staff, please show that you have completed this exercise by emailing your encrypted file to researchsupport@poverty-action.org.

Remember, do not send any file that contains any kind of PII from your project.

Please continue reading these slides for a few more tips!

A few more Boxcryptor tips

Inheritance and Boxcryptor

Encryption properties and permissions are inherited from the parent folder. If you add a file to an encrypted shared folder, the persons who you shared the folder with can access all encrypted files inside the folder, too.

Blue Lock: Encrypted and permission to access for Person 1

Red Lock: Encrypted and permission to access for Person 2

Blue and Red Lock: Encrypted and permission to access for Person 1 and Person 2
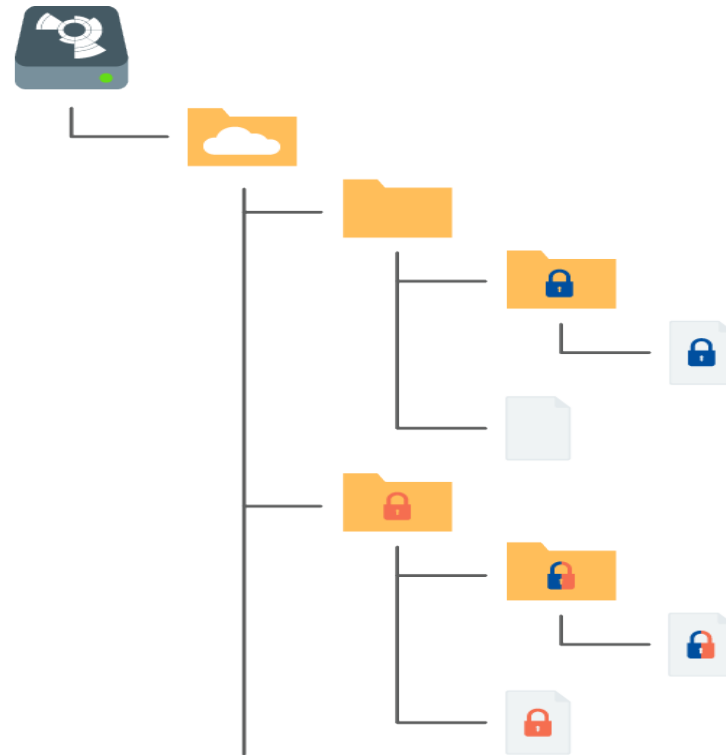
Recognizing Encrypted Files

Boxcryptor allows you to have **encrypted and unencrypted** files and folders. All files and folders in the Boxcryptor drive are **marked with small icons** that indicate their current state.

Encrypted and synchronized

Not encrypted and synchronized

Encrypted and synchronization in progress

Not encrypted and synchronization in progress

Encrypted and synchronization failed

Not encrypted and synchronization failed

J-PAL
ABDUL LATIF JAMEEL POVERTY ACTION LAB

Boxcryptor Tips

- ## File/folder management

  - Remember "adding location" does NOT encrypt the folder – you must encrypt a folder within that location

  - Boxcryptor will resync ALL data and files if a new person is added to folder permissions later

  - Removing and encrypting only PII can avoid annoying re-sync of huge files

  - A file encrypted through Boxcryptor can be opened in Box (if they are synced)

  - Do not accidentally email files from the X: drive, as they will be unencrypted (attach from original location)

- ## Account/password management

  - Free accounts: don't forget your Boxcryptor password or you will lose all of your data

  - Institutional accounts: still share permissions with 1+ accts, INCLUDING boxcryptoradmin@poverty-action.org

  - Use IPA's institutional Boxcryptor account to avoid the above problems

J-PAL
ABDUL LATIF JAMEEL POVERTY ACTION LAB

Questions?

IPA staff can email support@poverty-action.org or visit the Global Help Desk.

Non-IPA staff can visit the Boxcryptor website.

If you are viewing these slides as part of a training, please send any questions through the training's support channels, such as Slack or email.