

Encryption Guidance

January 2021



CAVEATS

There is a great variety of encryption methods available depending on your computer configuration; this guide does not cover every single method available and many of you have found your own solutions.

We recognize this guide offers limited solutions and there are frequent issues with encryption tools. As a result, we are advocating and working for more sophisticated encryption tools. This guide is an important first step in demonstrating the critical need to protect University data.

Contact the appropriate compliance partner (e.g. Export Control or HIPAA) for guidance on the encrypting level requirements in the regulations. For technical assistance contact your Unit's IT Manager or the 24/7 IT Support Center.

Topics covered

- Email
- Drives
- Documents
- File Folders
- Stache
- UA Box Health
- Questions?

Digital Signature vs. Encryption

Encryption scrambles data to protect it and reduce the ability of unauthorized parties to understand the information.

Digital signatures bind the identity of the message sender to the message, ensuring integrity, messages authentication, and non-repudiation, whereas encryption provides confidentiality.

Use of digital signature may prevent encryption.

Why is Encryption Important?

- Legally required for data subject to HIPAA and export control regulations
- Makes information more difficult to intercept and steal
- Following the requirements prevents significant fines

In 2019, The University of Rochester Medical Center (URMC) was fined \$3 million by The Department of Health and Human Services' Office for Civil Rights (OCR) for failing to encrypt mobile devices and other HIPAA violations.

<https://www.hipaajournal.com/lack-of-encryption-leads-to-3-million-hipaa-penalty-for-new-york-medical-center/>

Encrypting Email

EMAIL CAVEATS

- **Always send an encrypted test message before sending restricted data to ensure the tool is properly working.**
- **Do Not E-mail Controlled Unclassified Information (CUI).**
- CUI needs to be shared and contained in the S3 bucket.
- **Do not use your student or personal Gmail to send encrypted export control or HIPAA files.** The encryption level is not sufficient to comply with federal regulations.
- Students working on export control or HIPAA projects will need a Catworks (Outlook) account to email or receive restricted data.

Outlook Encryption Restrictions

Limitations: The following cannot encrypt

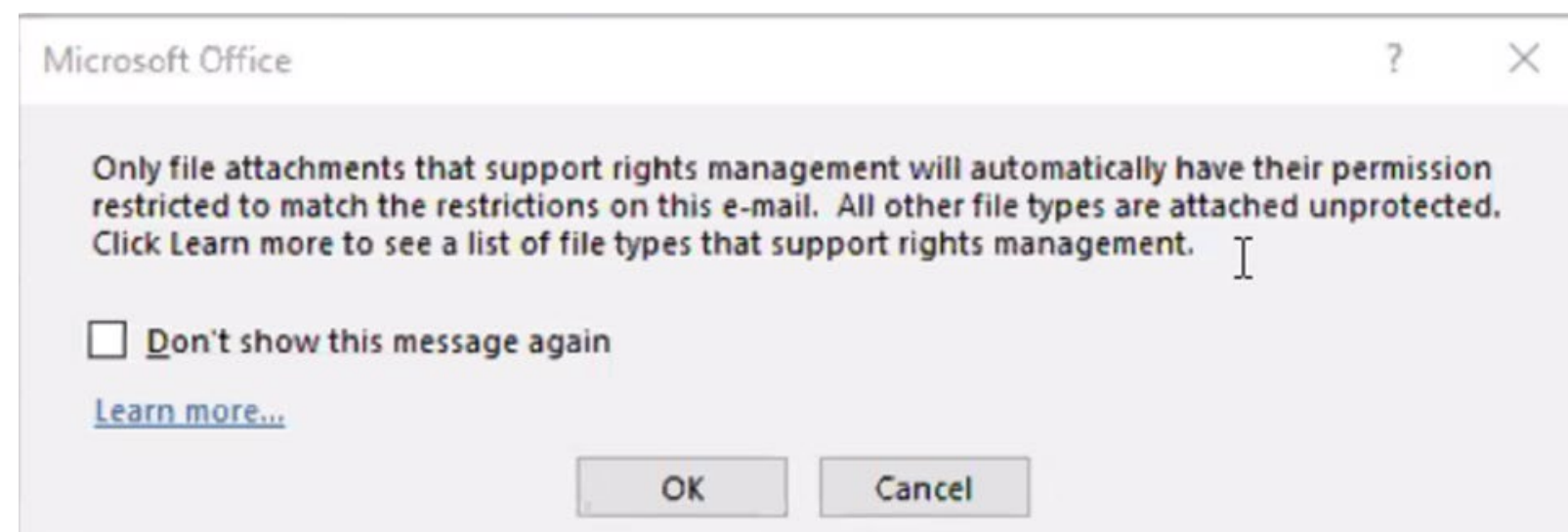
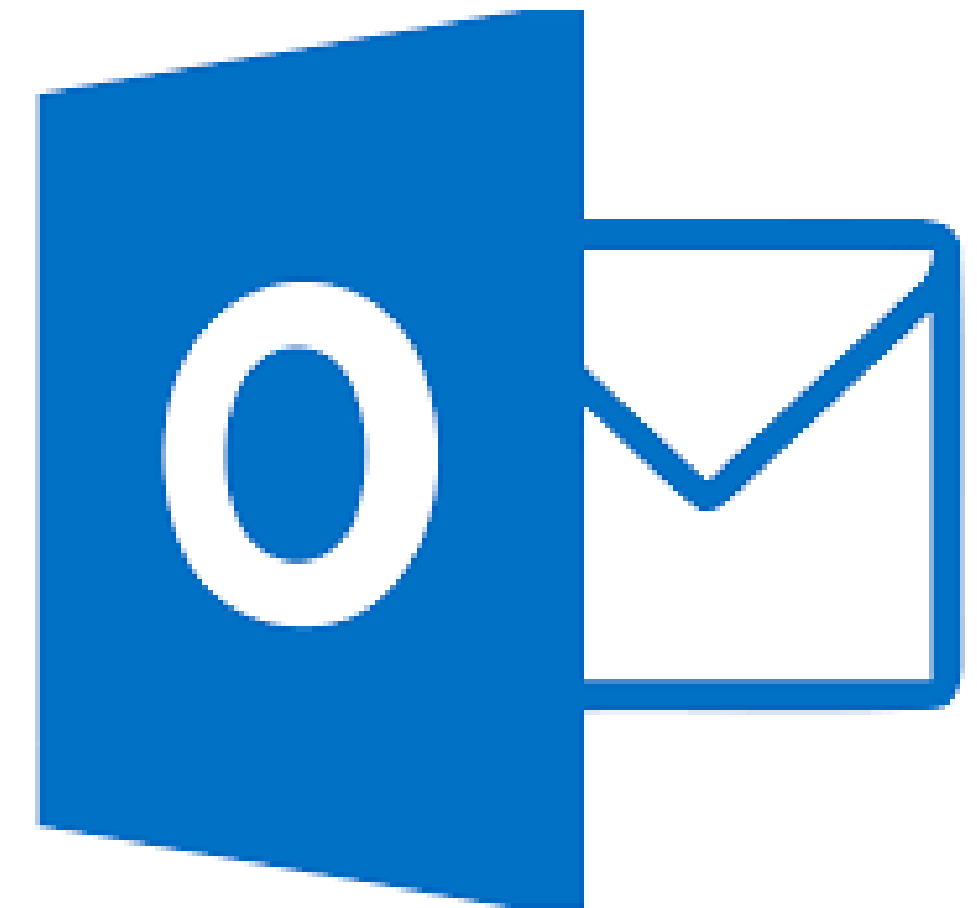
Emails with a **digital signature**

Messages **larger than 30Mb**

OneDrive for Business attachments

File attachments: .lnk, .exe, .com, .cmd, .bat, .dll, .ini, .pst, .sca, .drm, .sys, .cpl, .inf, .drv, .dat, .tmp, .msg, .msp, .msi, .pdb, .jar

Folder attachments: Windows, Program Files (\Program Files and \Program Files (x86)), \ProgramData, \AppData (for all users)

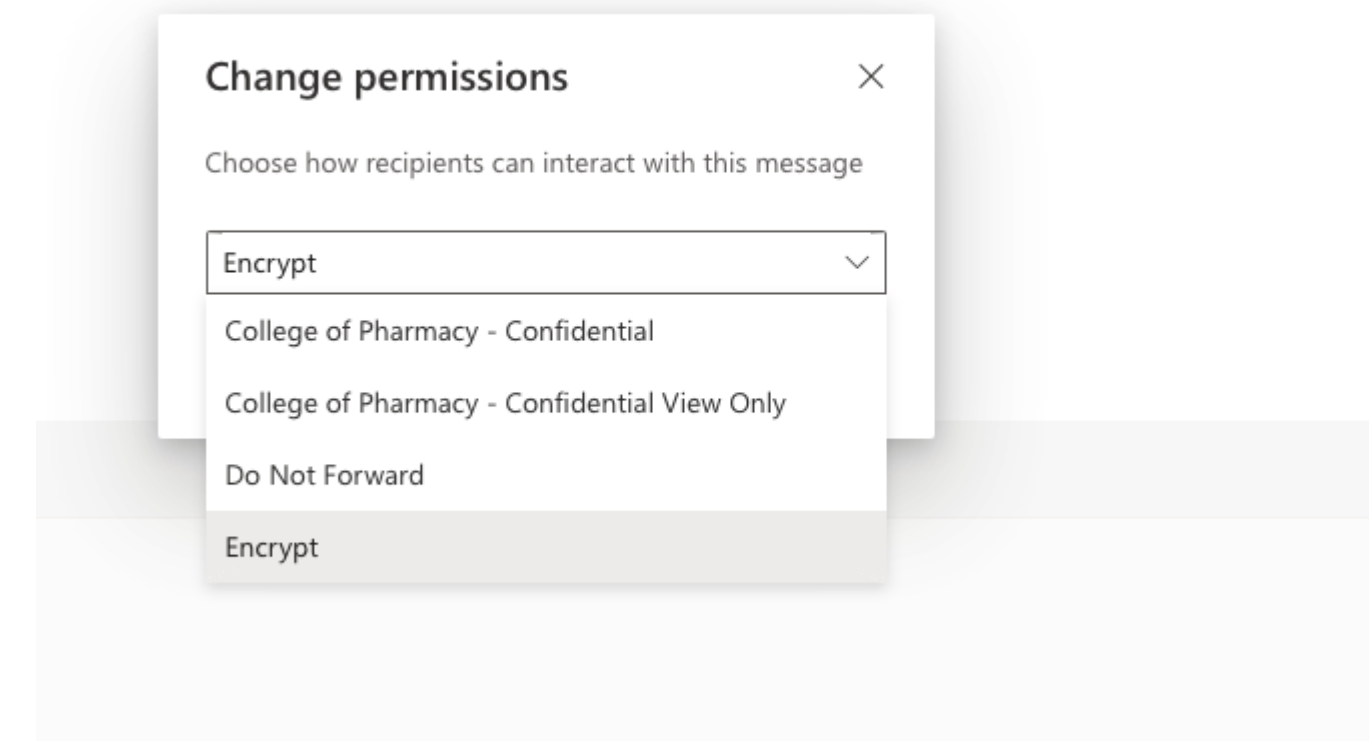
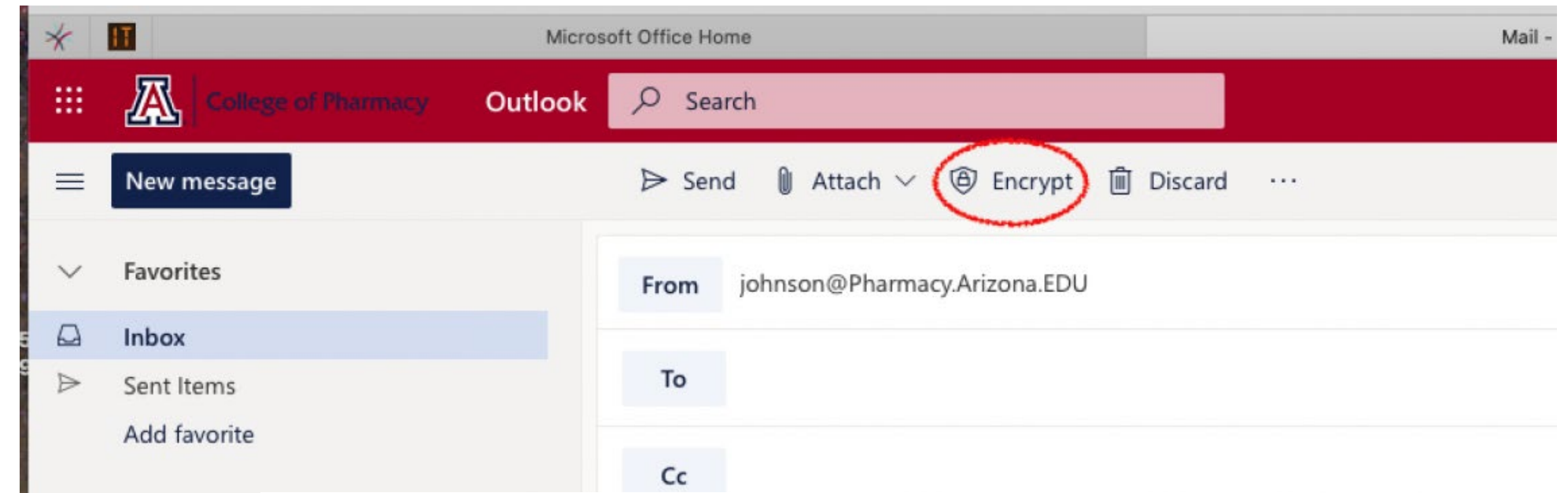


Sending Encrypted Email in Outlook Online (O365)

STEPS

1. Click “**encrypt**” at top of message, near “send”
2. **Confirm encryption:** message above “From”:
“Encrypt: This message is encrypted....”
3. **Permission levels** can be changed at the end of encryption message:

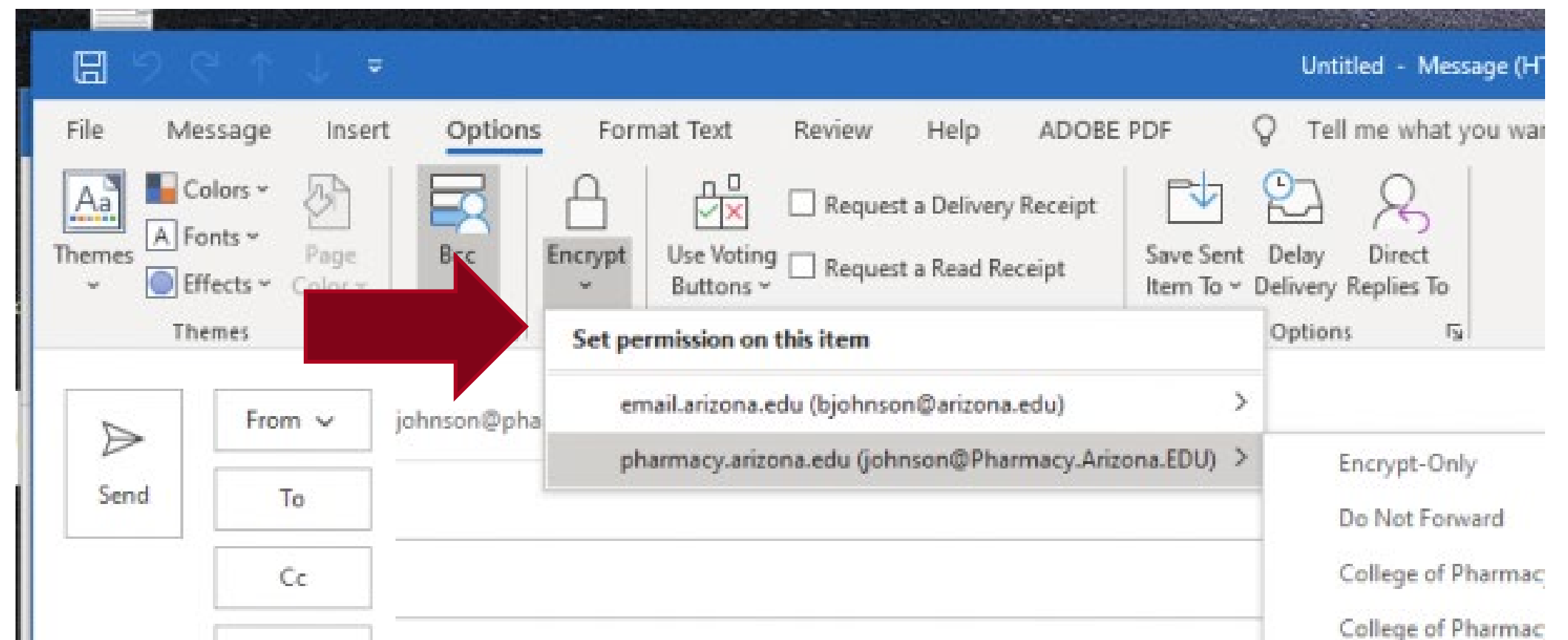
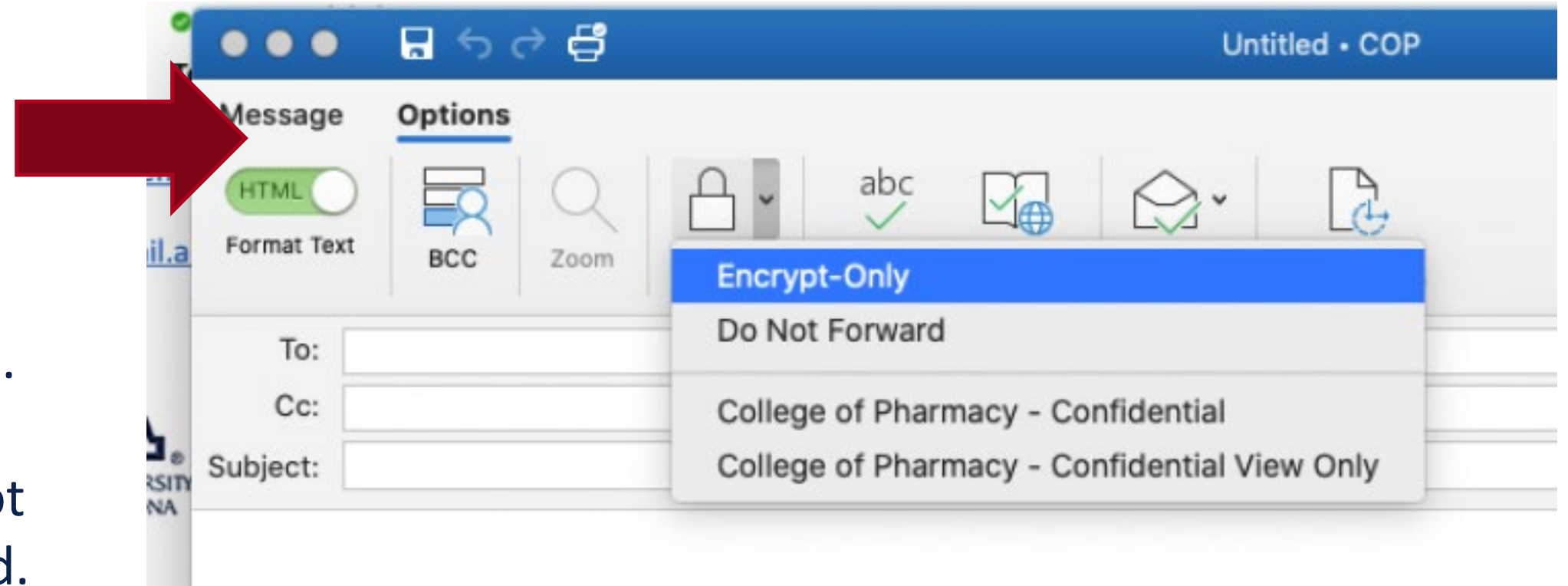
- **Encrypt:** Recipients can’t remove encryption.
- **Do Not Forward:** Message can be read, but cannot be forwarded, printed, or have its contents copied.
- **University of Arizona – Confidential:** Content can be modified but cannot be copied and printed.
- **University of Arizona – Confidential View Only:** Content cannot be modified.



Sending Encrypted Email in Outlook Desktop Application

STEPS

1. Click “**Options**” in toolbar, select “**Encrypt**”
2. Options for encryption:
 - **Encrypt Only:** Recipients can’t remove encryption.
 - **Do Not Forward:** Message can be read, but cannot be forwarded, printed, or have its contents copied.
 - **University of Arizona – Confidential:** Content can be modified but cannot be copied and printed.
 - **University of Arizona – Confidential View Only:** Content cannot be modified.



Sending Encrypted Email Using Subject Line Encryption

Works with Outlook Online & Desktop App

STEPS

Simply type [encrypt] or [secure] in the subject line.

IMPORTANT! This is case sensitive and not recommended as mistakes are more likely.

<https://it.arizona.edu/documentation/uconnect365-email-encryption>

- **Examples: will encrypt:**

- Subject: Game day plans [encrypt]
- Subject: [secure] Game day plans
- Subject: Game day [encrypt] plans

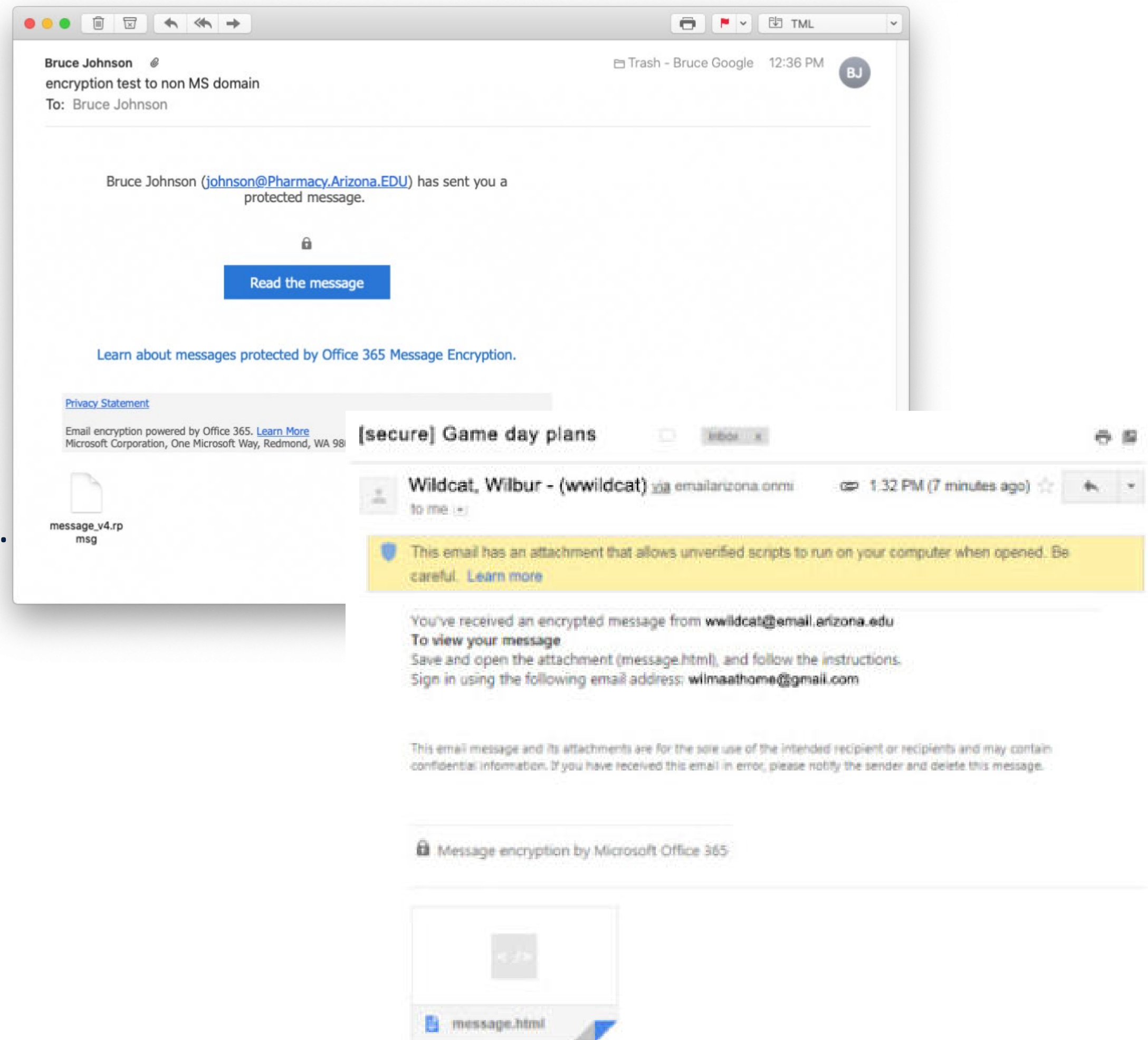
- **Examples: will not encrypt:**

- Subject: [Encrypt] Game day plans
- Subject: Game day plans [SECURE]
- Subject: encrypt: Game day plans
- Subject: [secure:] Game day plans

Receiving Encrypted Email

What do external recipients see?

- Recipients receive a message with directions to access the encrypted email.
- Upon clicking “**Read the Message**” they are directed to a page with two options: Sign in with Google or Sign in with one-time passcode.
- **Sign in with Google** allows use of Gmail account to access the message.
- **Sign in with a one-time passcode** asks for the recipient’s email address to which a code is sent to open the email.



Internal recipients will see a message indicating the message is encrypted.

Encrypting Drives

Windows 10 & Mac OS X

TPM – Trusted Platform Module

A computer chip that is part of the computer motherboard, the TPM provides hardware-based, security related functions such as carrying out cryptographic operations.

To make use of BitLocker, your device must have a TPM.

BitLocker & Windows Version

The Home version of Windows installed on *most* consumer grade computers cannot use BitLocker.

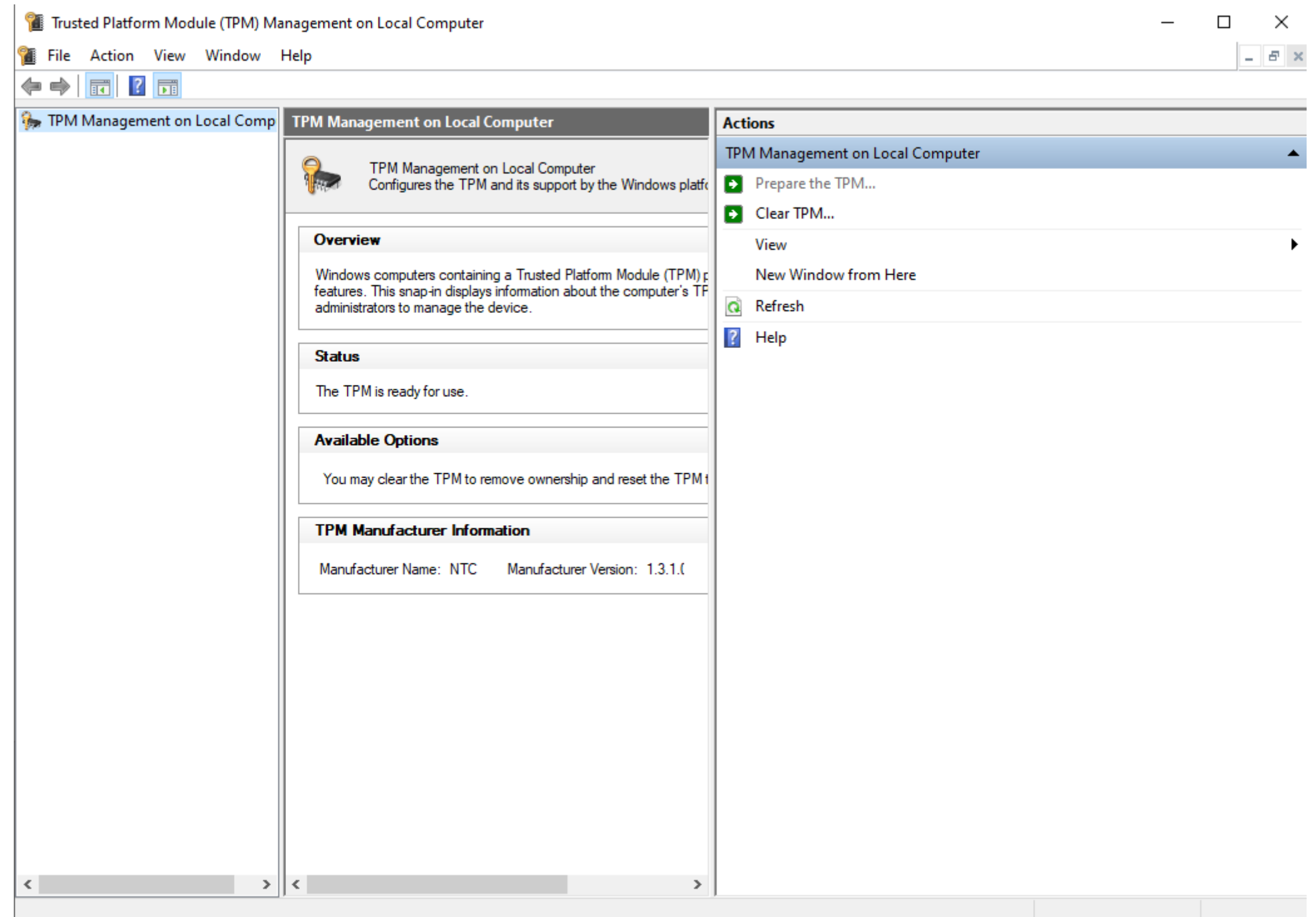
If you have a TPM and the Home version of Windows, there are other methods of encrypting your hard drive.

Checking if your Computer has a TPM

Windows 10

STEPS

- Press “**Windows Key + R**”.
- Type “**tpm.msc**” in the open text field and press enter.
- If you do not have a TPM, you will see “*Compatible TPM cannot be found*”.
- If you have a TPM you will see the window on the right.

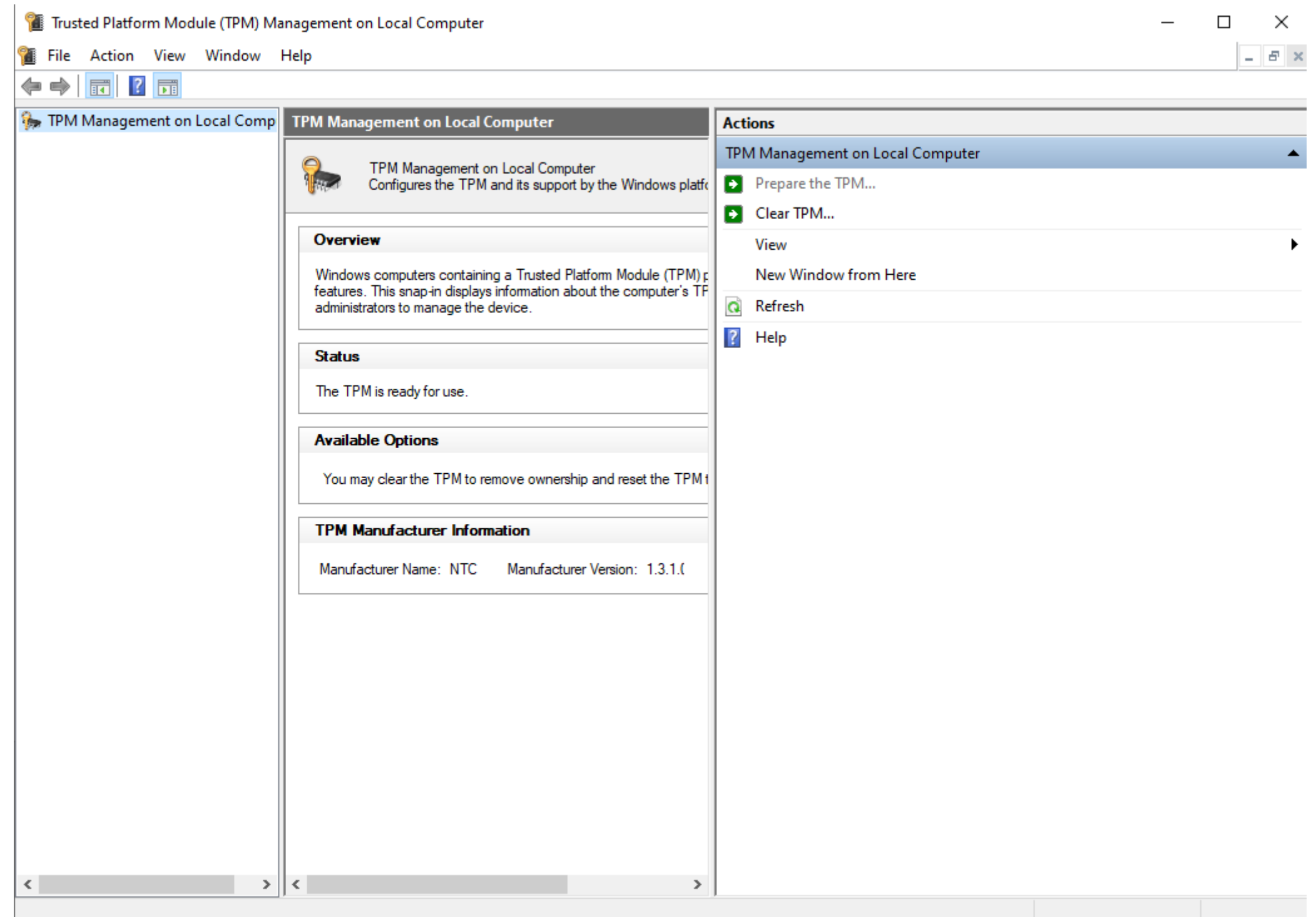


How to Turn on TPM

Windows 10

STEPS

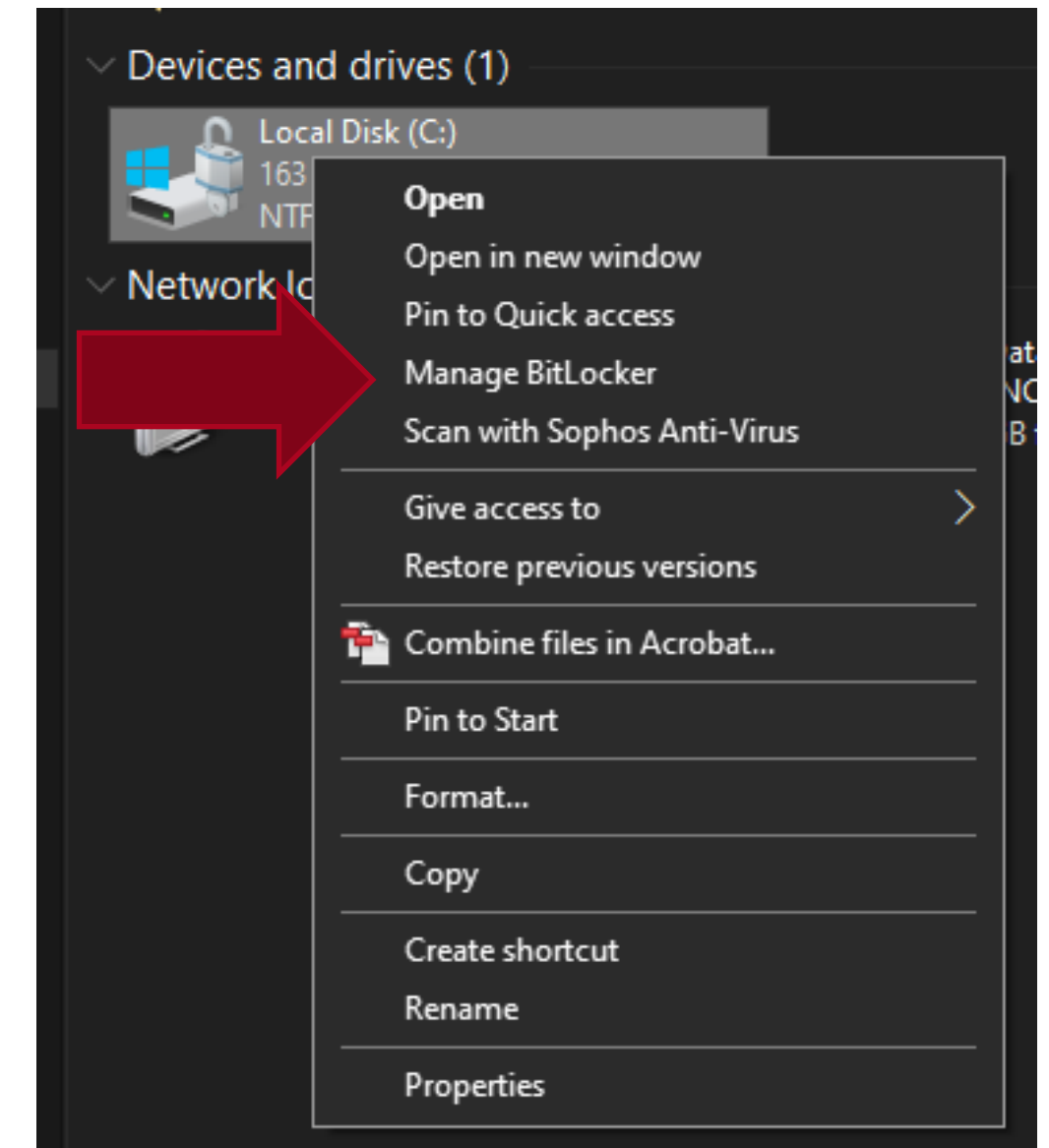
1. Press the “**Windows Key + R**” and type “**tpm.msc**” to open the TPM Management Console.
 2. In the Action pane, click “**Turn TPM On**” or “**Prepare the TPM**”, to open a new window. *Please read the message that appears.*
- **Shutdown or restart** your computer and **follow the prompts.**



Encrypting Drive in Windows 10 (Not Home)

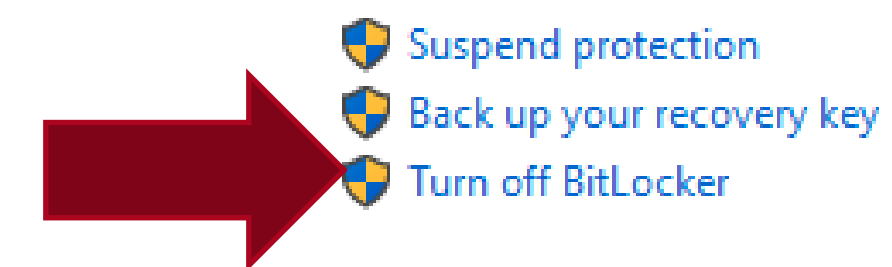
STEPS

1. Press “**windows key + e**” and locate the drive to encrypt.
2. **Right click on the local disk drive to encrypt and select “Turn on Bitlocker”**.*
3. Choose “**Enter a Password**”.
4. Select “**How to Enable a Recovery Key**” and follow prompts.
5. Choose “**Encrypt Entire Drive**”, the most secure method.
6. Select “**Start Encrypting**” to begin.



Operating system drive

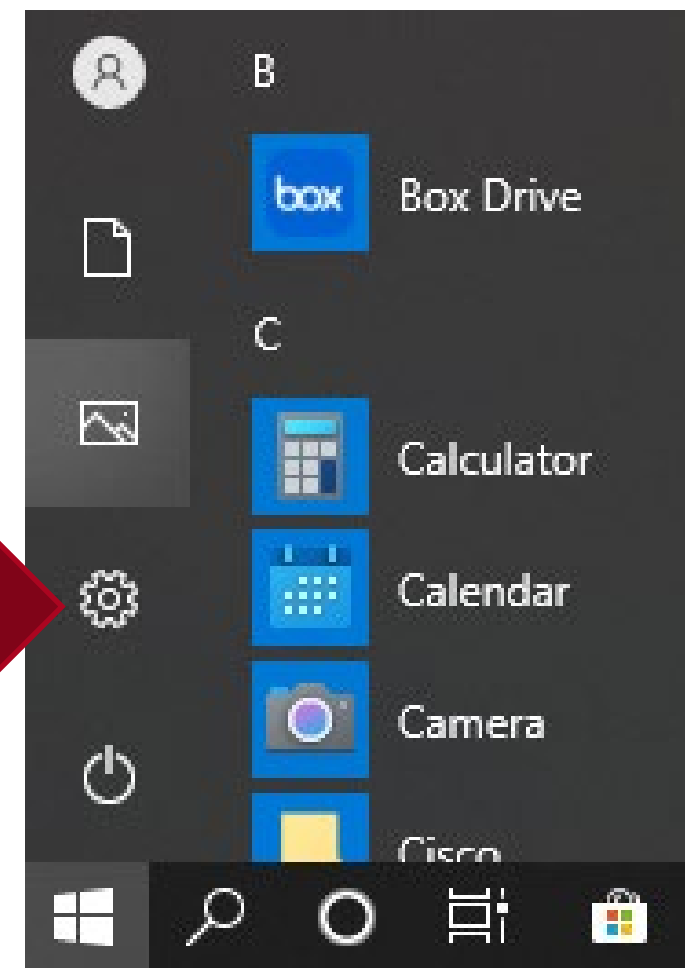
C: BitLocker on



Encrypting Drive in Windows 10 (Home)

STEPS

1. Open the “**Start Menu**” and click “**Settings**”.
2. Click “**Updates & Security**”.
3. Click “**Device Encryption**”, towards the bottom of the list on the left.
4. Click “**Turn On**”.



Device encryption


Device encryption helps protect your files and folders from unauthorized access in case your device is lost or stolen.

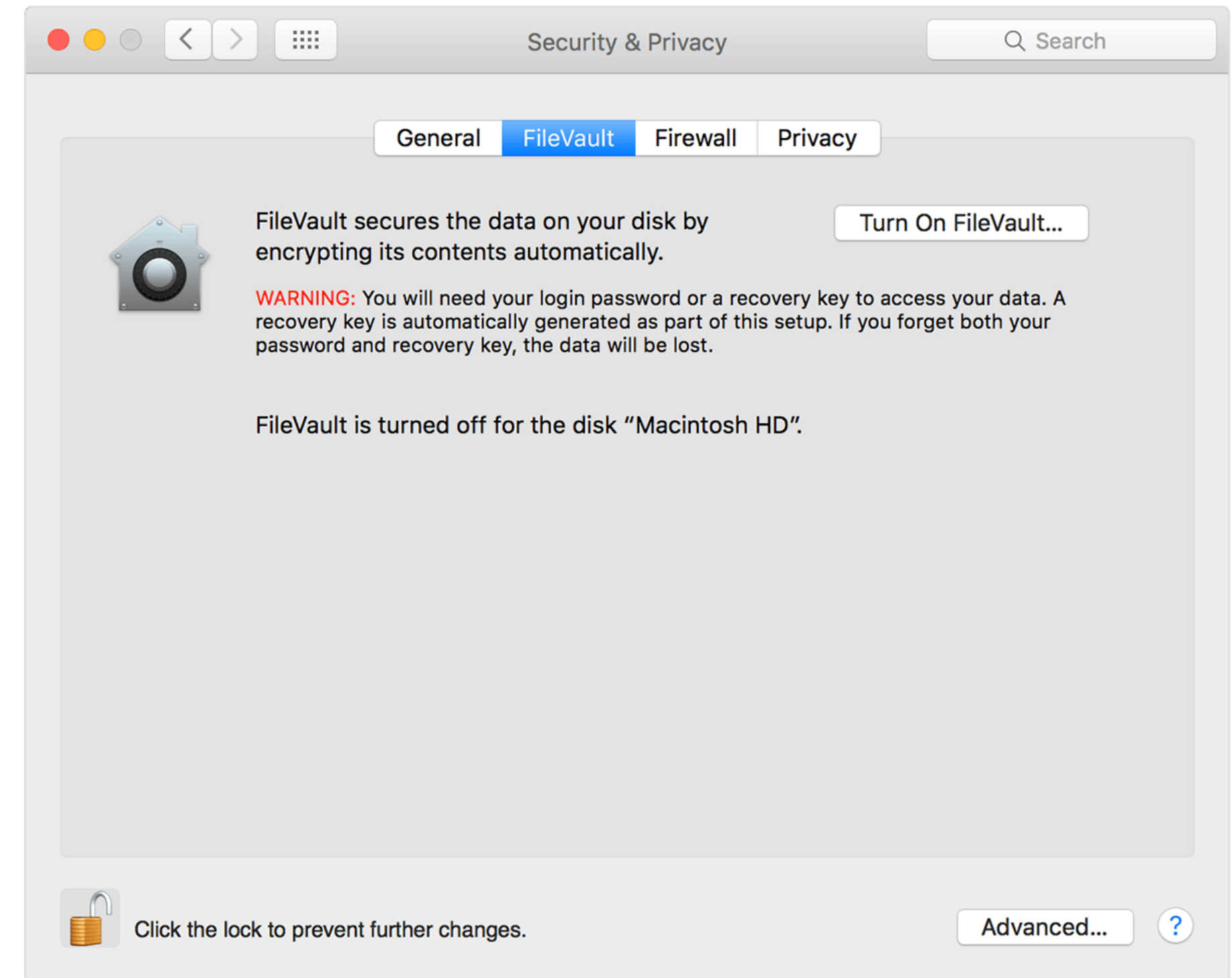
Device encryption is off.

Turn on

Encrypting Drive in Mac OS X

STEPS

1. Choose Apple menu  and click “**System Preferences**”, then click “**Security & Privacy**”.
2. Click the “**FileVault Tab**”.
3. Click  , then enter an administrator name and password.
4. Click Turn On “**FileVault**”.
5. Choose how you would unlock your disk and reset your password, in case it is forgotten.



Encrypting Documents & Folders

Windows 10 & Mac OS X

You Should Know!

Best Practices

- Encrypt your entire disk drive.
- Use e-mail encryption. **Send encrypted TEST messages before emailing restricted data.**
- *Encrypting single files or folders is not a replacement for encrypting your entire disk drive or using e-mail encryption.*



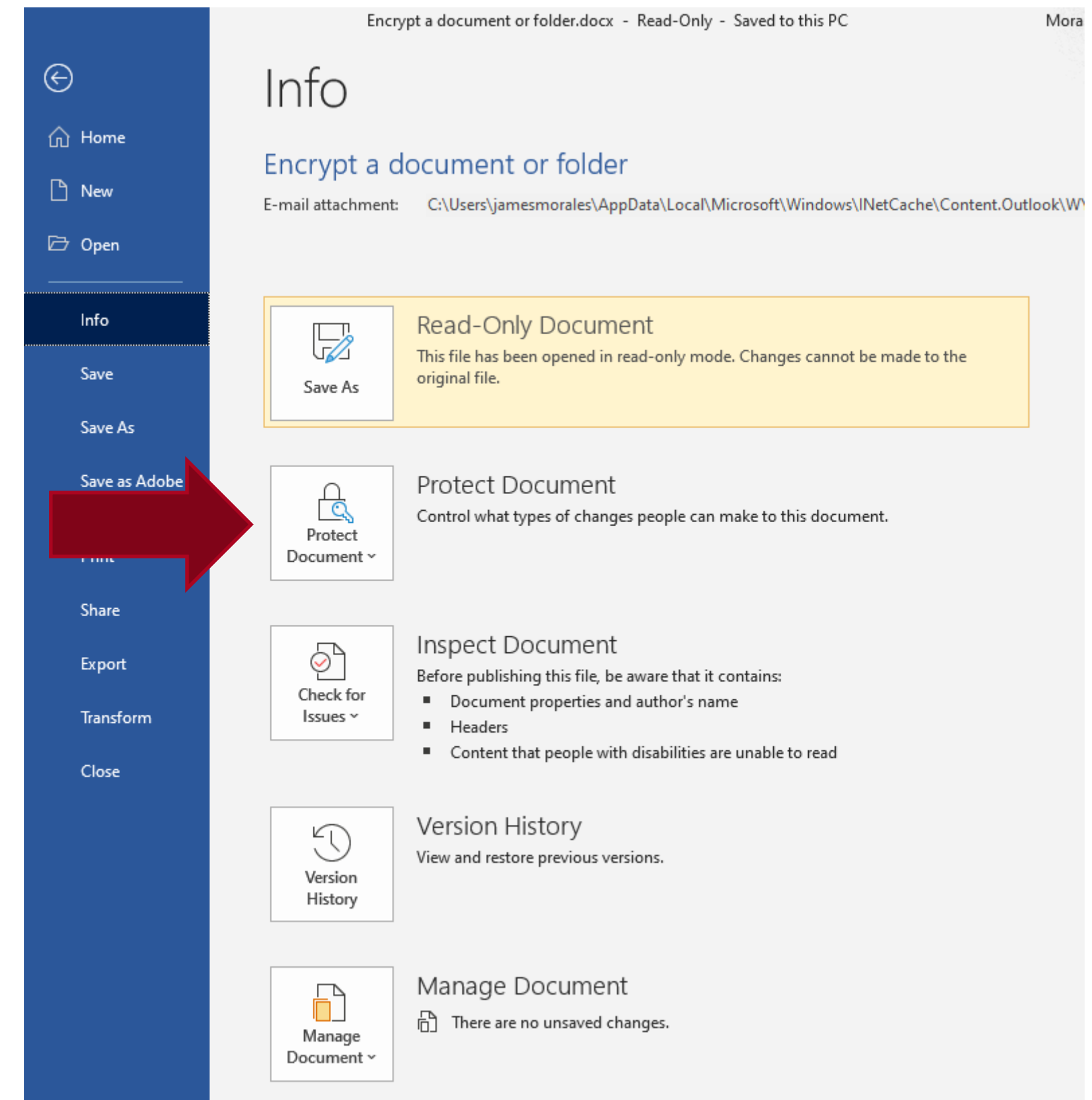
IMPORTANT

Encrypting Documents in Microsoft Office Suite

Word, Excel, PowerPoint, etc.

STEPS

- Open the document.
- Click “**File**” in the top left of the window.
- Click on “**Info**”.
- Select “**Protect [Document]**”.
- Click “**Encrypt with Password**” and enter password.
- Use encrypted email to send encrypted document as an attachment. Provide password separately.



Encrypting PDFs in Adobe

Acrobat DC

STEPS

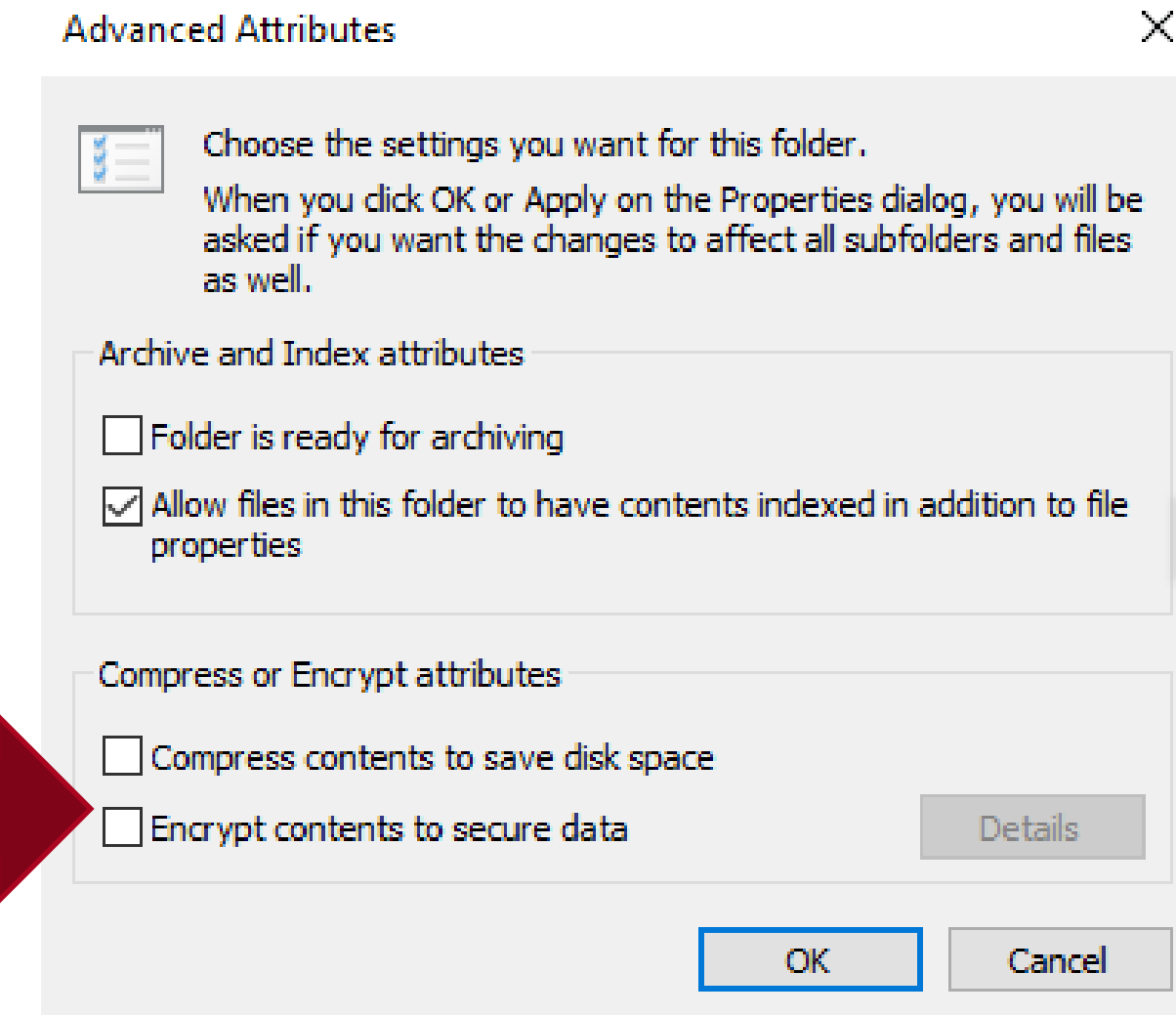
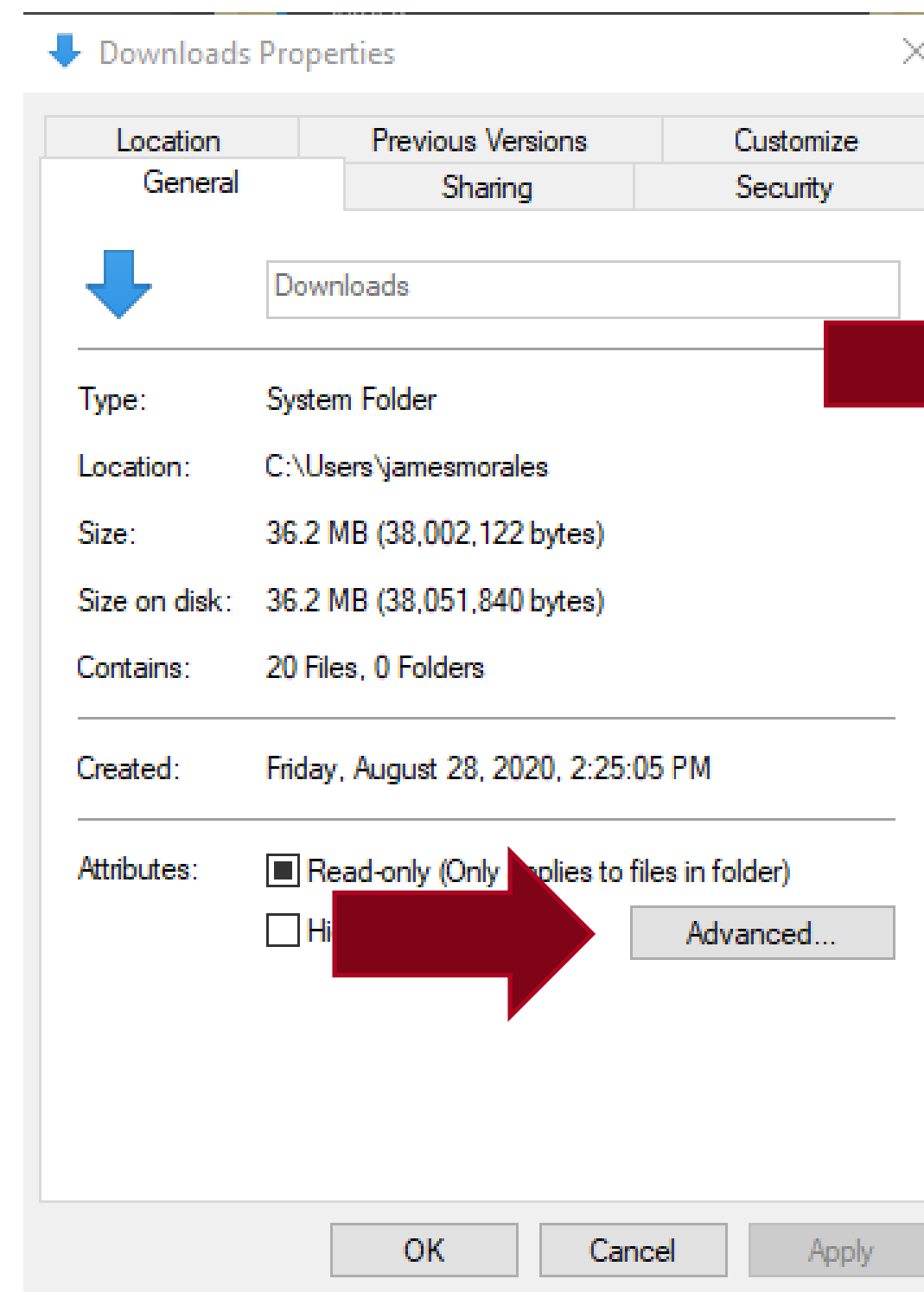
- Open PDF with Adobe Acrobat DC.
- Navigate to “**Tools**” at the top of the window.
- Scroll down and click “**Protect**” under “**Protect & Standardize**”.
- A new toolbar at the top of the document offers a variety of options.
- Click “**Protect Using Password**”, select the options and enter a new password.

The image shows a sequence of steps in Adobe Acrobat DC. At the top, the 'Protect & Standardize' panel is visible, with a red arrow pointing to the 'Protect' icon. Below this, the main toolbar is shown with the 'Protect' tool selected. The 'Protect Using Password' dialog box is open, showing options for 'Viewing' and 'Editing', and fields for 'Type Password' and 'Re-type Password'. The 'Apply' button is highlighted.

Encrypting Folders in Microsoft Windows 10

STEPS

- Navigate to the location of the folder and right click on the folder that you want to encrypt.
- Select **“Advanced”**.
- Check the box **“Encrypt contents to secure data”**.
- Click **“OK”**.



Stache



Password Storage

Stache

What is Stache?

A secure backup of sensitive data including encryption keys, passwords, passphrases, and personal identification numbers.

Provides views of stored, shared, and digital certificate entries.

<https://stache.arizona.edu/>



Stache

Steps for using Stache

1. Go to <https://stache.arizona.edu>.
2. Log in with your **UA NetID** and **password**.
3. Select **new entry**.
4. In the **nickname** field, enter a name that will remind you of the information you are storing. This field is not encrypted, so do not put any sensitive information (such as your password) here.
5. The next three fields (**purpose**, **secret**, and **memo**) are all encrypted, so you can put sensitive data in them. The lock icon next to these fields indicates that their contents will be encrypted. You do not have to use all three fields.
6. Enter any username and password information and any login details that you want to store.
7. If you want to share a password with another faculty or staff member (you should never do this with your UA NetID password), enter their NetID in the **Share with...** field.
8. You can use the **add tags** field if you want to later search by category although this is not necessary. This field is not encrypted.
9. **Save** the entry.
10. You will be redirected to your main Stache site, where you can see all of your entries. Entries that you have created are blue, while entries that have been shared with you are green.

UA Box Health

UA Box Health

Information

- HIPAA compliant secure cloud storage solution.
- Requires training prior to use (HIPAA Privacy Program).
- Box Health training program includes instructions on how to use Box Health.

The screenshot displays the 'UA Box Health Training' interface. At the top left is the University of Arizona logo. Below it is a 'Menu' section with a dropdown arrow and the text 'UA BOX Health Training Module-T...'. The menu items are: 'UA BOX Health' (highlighted), 'Navigation Instructions', 'About UA Box Health', 'Learning Objectives', 'What is UA Box Health', 'UA BOX Health Storage Guidance', 'About UA Box Health', 'Remember', 'Understanding Folder Ownership', 'UA Box Health Naming Conven...', 'Official Box Apps', 'Box Tools', 'Box Sync', 'Collaborators & Sharing', 'Training and Certification', 'UA Box Health Audits', 'Summary', 'UA BOX Health Training Compl...', and 'Questions?'. The main content area features the title 'UA BOX Health User Training Module' and a large blue box with the 'box' logo. At the bottom center is a red triangle with the University of Arizona logo. The bottom right corner has navigation buttons: '< PREV' and 'NEXT >'. A speaker icon is visible in the bottom left corner of the interface.

Other resources/references

Resources

- ISO [Encryption Guideline](#)
- [Classification Standard](#)
- <https://it.arizona.edu/documentation/uaconnect365-email-encryption>
- <https://it.arizona.edu/documentation/email-encryption>

Thank you for helping to keep our
restricted data secure!

