

Analytics Boot Camp

March 29, 2017

Data Security & HIPAA



hfma[™] metropolitan philadelphia chapter
healthcare financial management association

Contact Information

Michael Rossi, CPA, FHFMA

Director of Government Reimbursement

Penn Medicine

267-414-2238

Michael.Rossi@uphs.upenn.edu



hfma[™]

metropolitan philadelphia chapter
healthcare financial management association

Disclaimer!!

All of the views expressed herein are mine and may not necessarily represent the views of my employer, the University of Pennsylvania Health System, its affiliates or the University of Pennsylvania School of Medicine.



hfma[™]

metropolitan philadelphia chapter
healthcare financial management association

Objectives

- Identify PHI data
- Protect PHI data
- Review Encryption Techniques
 - Temporary (WinZIP, ZIXmail)
 - Permanent (Bitlocker, TPM)



hfma[™]

metropolitan philadelphia chapter
healthcare financial management association

What is PHI?

- Established by Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Protected Health Information
 - individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.



hfma[™]

metropolitan philadelphia chapter
healthcare financial management association

18 Identifiers

- Name
- Address
- Birth, Admission, Discharge
- Telephone
- Vehicle IDs
- Fax Number
- Device IDs
- Email Address
- URL
- SS Number
- IP Address
- Medical Record Numbers
- Finger/Voice Prints
- Health Plan Numbers
- Full Face Photos
- Account Numbers
- Certificate/License Numbers
- Any Other Unique Number, Characteristic or Code



Protecting PHI

- March 3, 2017 – Sharp HealthCare (San Diego)
 - 757 Health Screening Records
 - Stolen Computer and “External Memory Device”
- February 23, 2017 – Allina Health (Minneapolis)
 - Documents from recycling bin thrown out before the physician could shred them
- February 23, 2017 – North Carolina Department of Health & Human Services
 - Sent private patient information to nursing homes by unencrypted email, affecting almost 13,000 Medicaid patients



Protected PHI or Not?

Data is found...

- On a desktop computer in office building with key card access
- On a USB drive carried from one office to another
- In a password encrypted ZIP file on a CD-ROM mailed to Medicare Contractor
- On a Google Drive



HIPAA Security Rule

- Focus on Electronic PHI (e-PHI)
- “maintain reasonable and appropriate administrative, technical, and physical safeguards”
 - Ensure confidentiality
 - Identify/Protect against *reasonably anticipated* threats
 - Protect against *reasonably anticipated*, impermissible uses
 - Ensure compliance by workforce



e-PHI Protection Toolbox

- Hardware Solutions
 - Desktop, Laptop
- Software Solutions
 - WinZIP, ZixMail
- Removable Media Solutions
 - CD-ROM
 - USB Drives

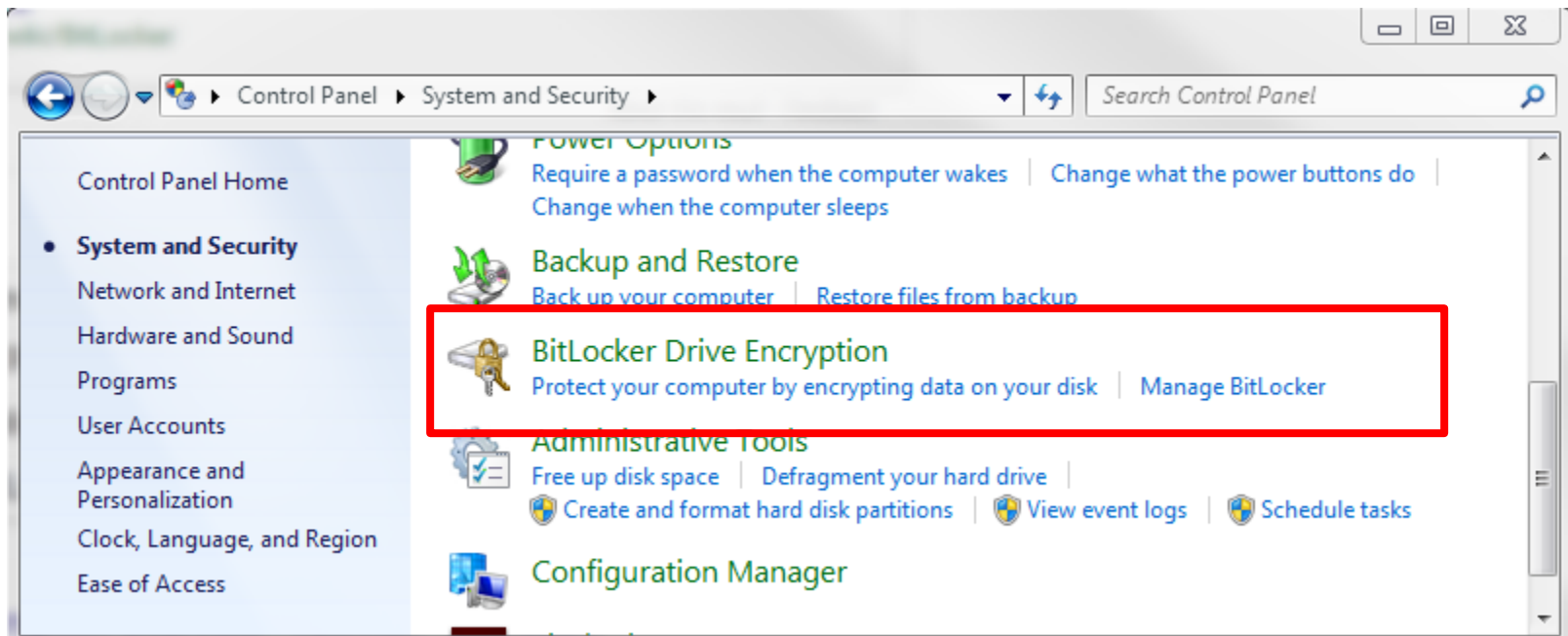


BitLocker & TPM

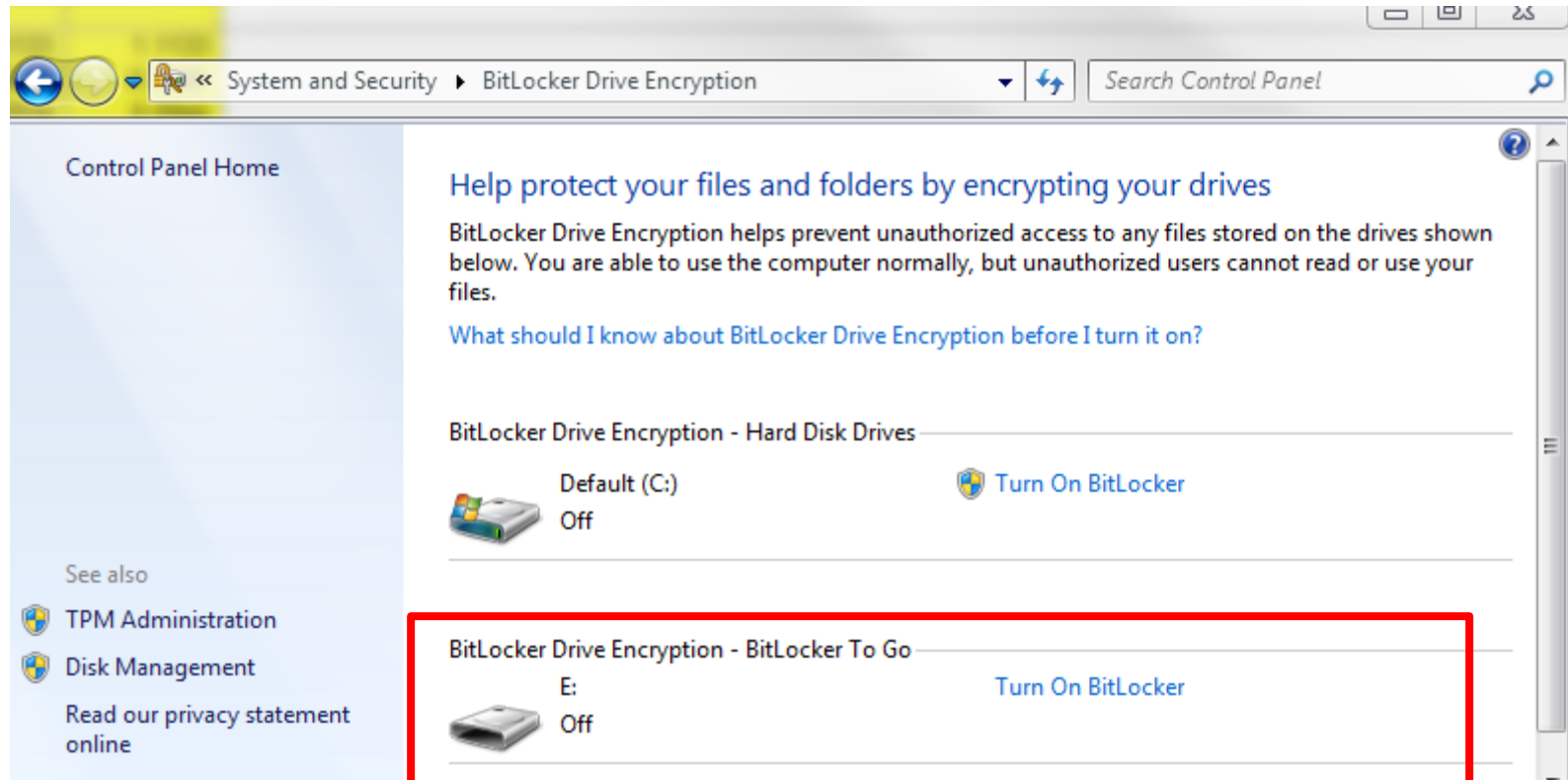
- Included with Windows Vista and Later
- PC Hardware must have a Trusted Platform Module (TPM)
 - Secure Cryptoprocessor
- Control Panel > System and Security > BitLocker Drive Encryption
- Encrypts the hard drive, requiring password to “unlock” drive
- Files copied from hard drive are NOT encrypted
- Can use to encrypt USB Flash Drives



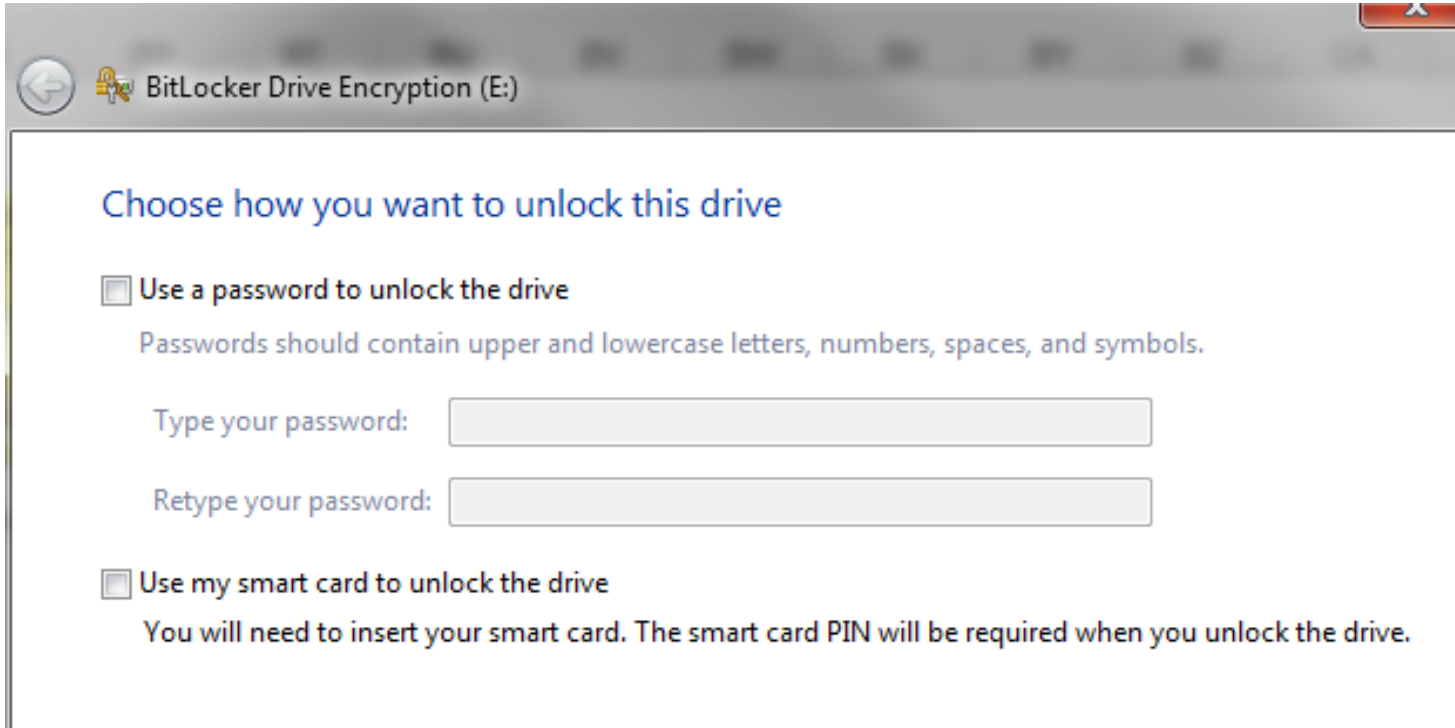
Activating BitLocker



Using BitLocker to Go



Using BitLocker To Go



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

☐ Use a password to unlock the drive

Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.

Type your password:

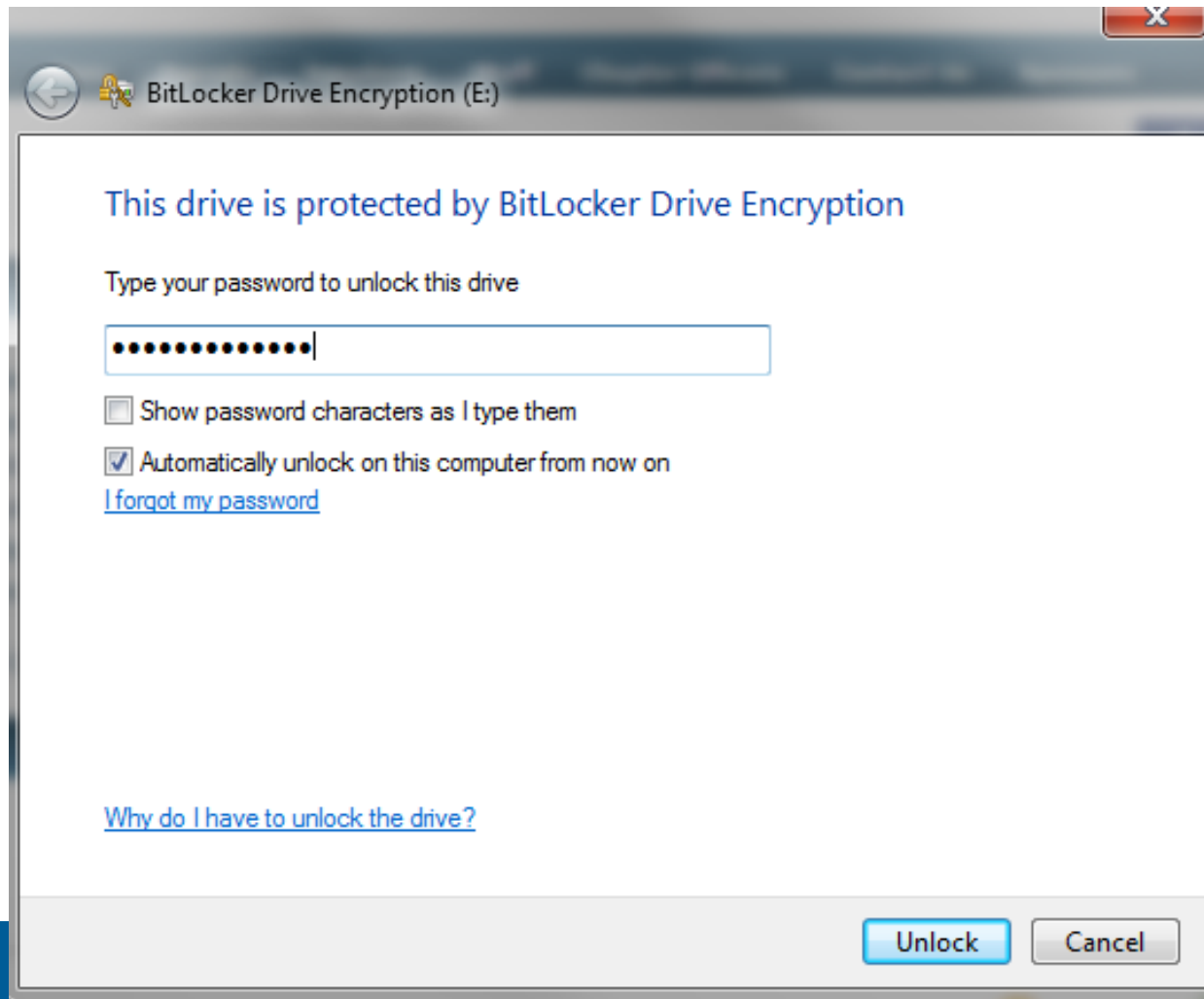
Retype your password:

☐ Use my smart card to unlock the drive

You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.



Using BitLocker To Go

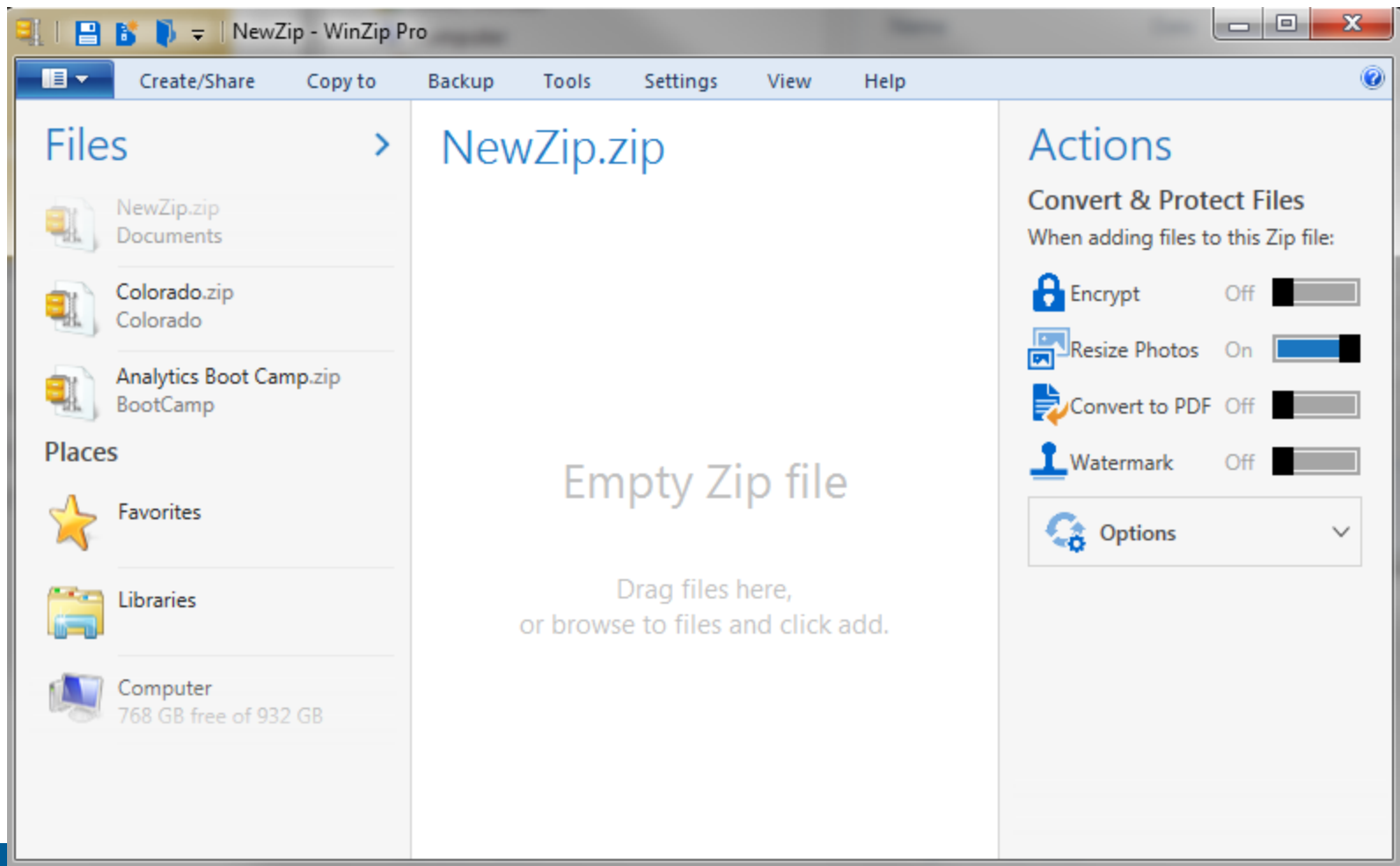


ZixMail & ZixGateway

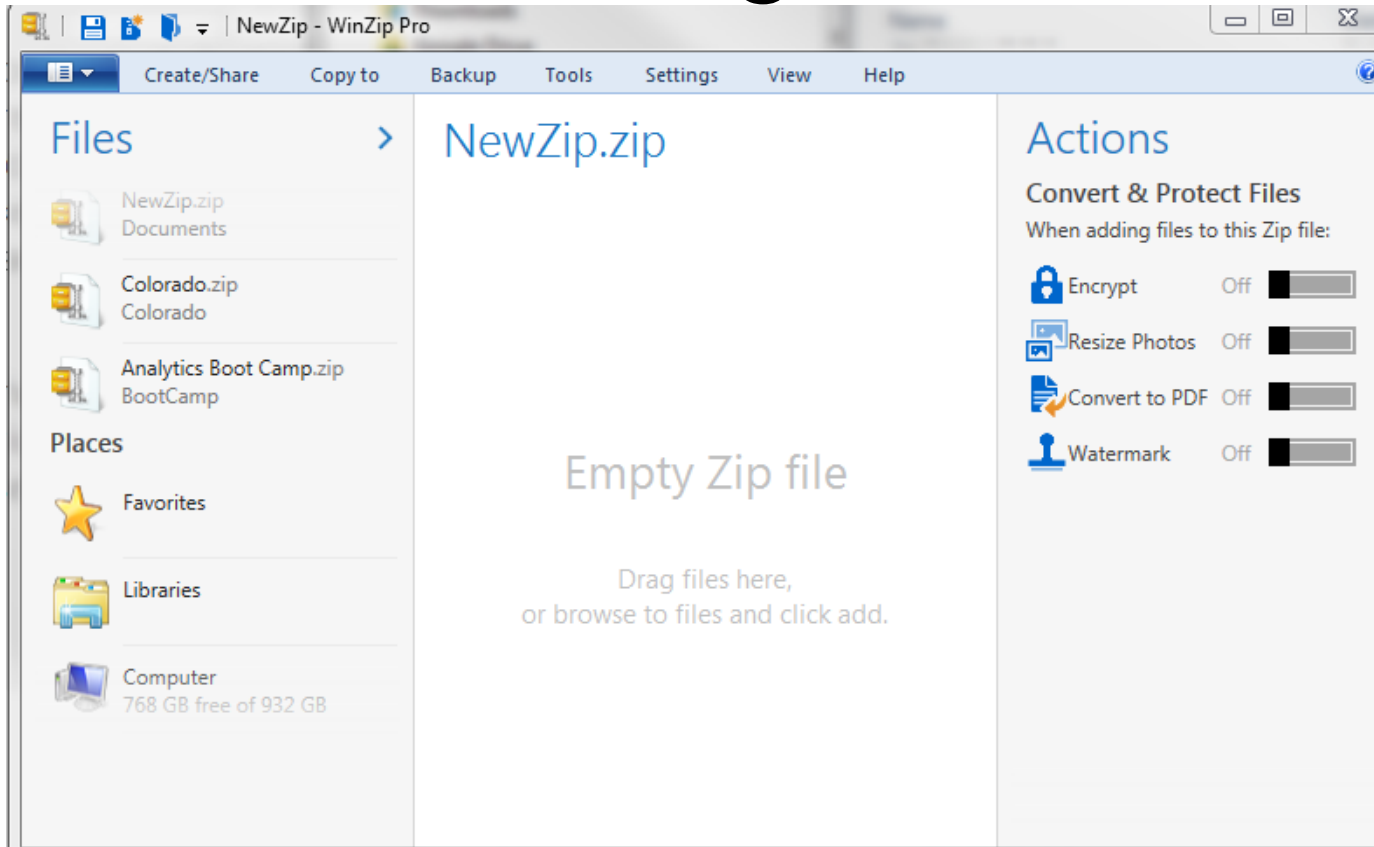
- End-to-end encryption of emails and attachments
- Single-Factor or Two-Factor Authentication
 - Something you know (password)
 - Something you have (token, one-time PIN)
 - Something you are (biometric)
- Desktop (ZixMail) and Server (ZixGateway)



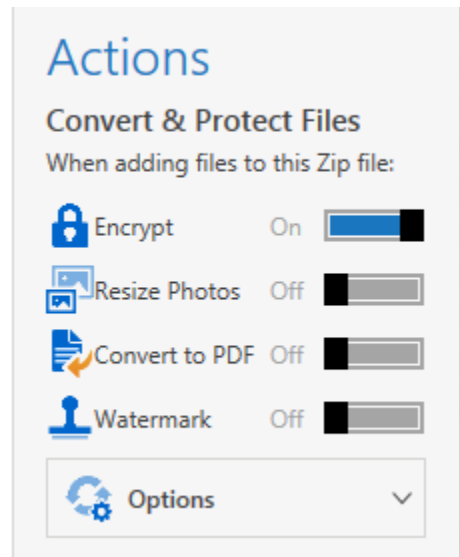
WinZIP



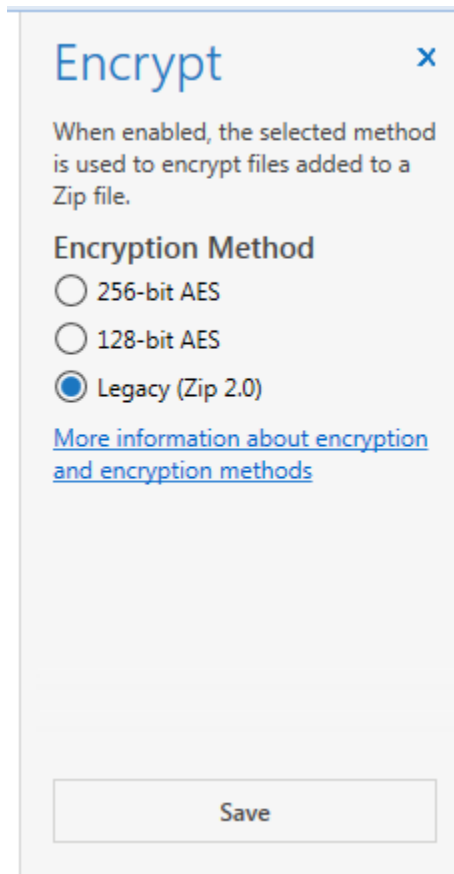
Creating a Secure ZIP



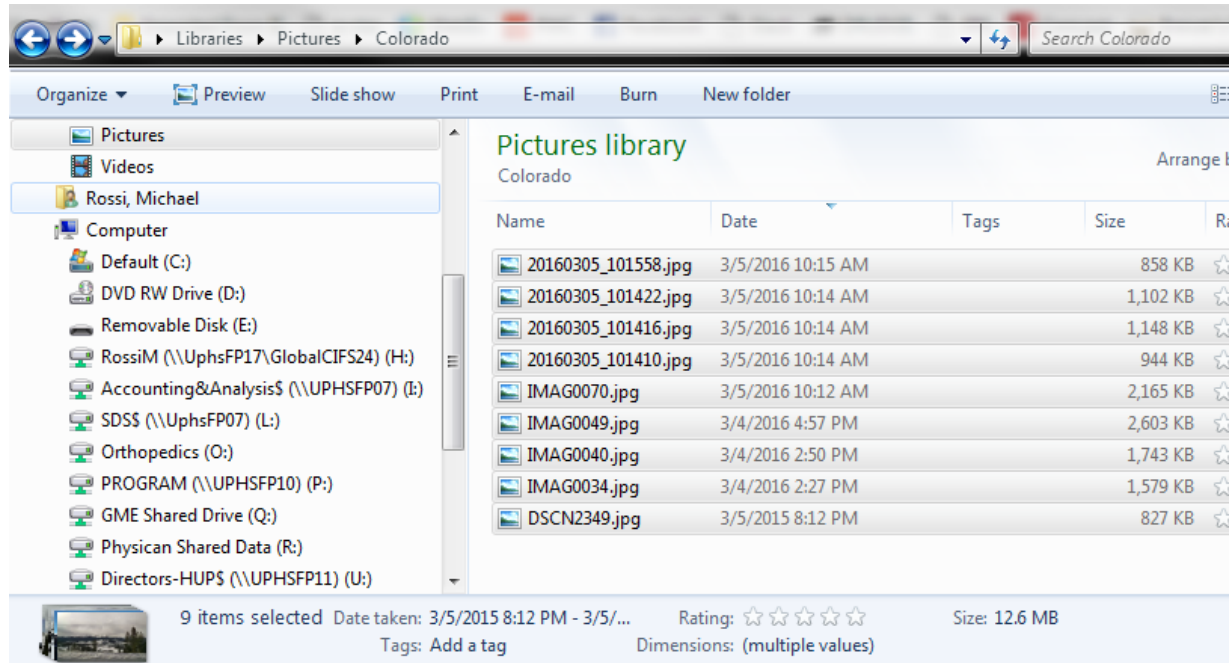
Creating a Secure ZIP



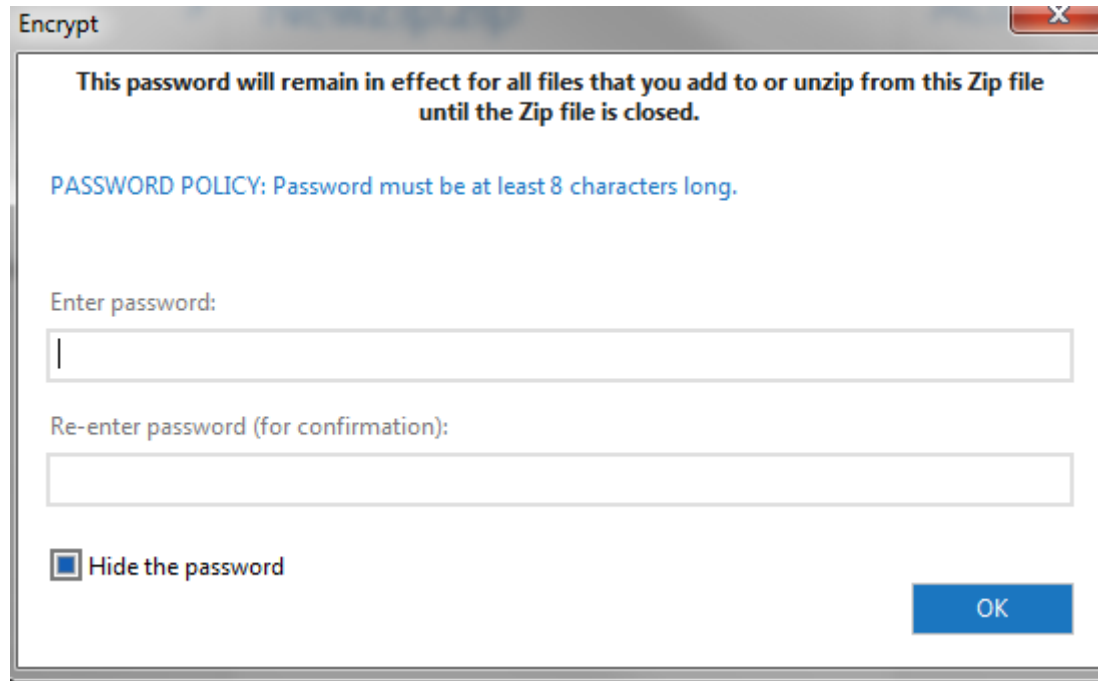
Creating a Secure ZIP



Creating a Secure ZIP



Creating a Secure ZIP

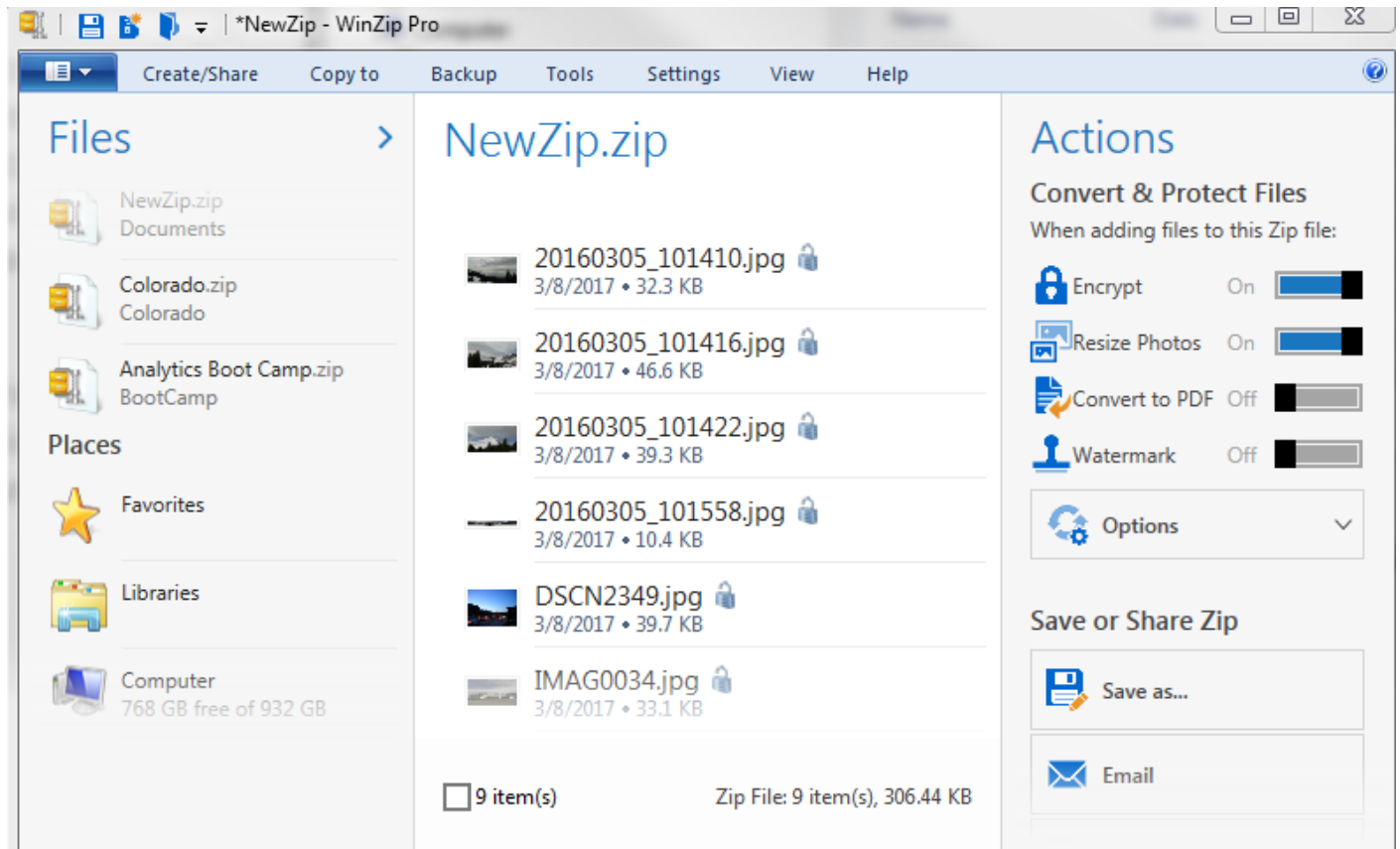


The image shows a standard Windows 'Encrypt' dialog box. At the top, the title bar reads 'Encrypt'. The main text area contains the following information:

- A warning: "This password will remain in effect for all files that you add to or unzip from this Zip file until the Zip file is closed."
- A password policy note: "PASSWORD POLICY: Password must be at least 8 characters long."
- A label "Enter password:" followed by a text input field containing a single vertical bar character.
- A label "Re-enter password (for confirmation):" followed by an empty text input field.
- A checkbox labeled "Hide the password" which is currently checked.
- An "OK" button in the bottom right corner.



Creating a Secure ZIP



Do's & Don'ts With Secure ZIP Files

- Email file & tell recipient to call for password
- Use a different password each time
- Email file and password for the file (together or separate)
- Use the same password each time

