Security

Robert Morris University | Pittsburgh, PA

Security Basics

Take some time to educate yourself on these security issues - vigilance is the best defense against system vulnerabilities!

How to Protect Your System

Ensure antivirus software is installed. It is crucial to make sure that any antivirus software is installed and up to date! Learn more about antivirus in the Sophos Antivirus section below.

Ensure that the firewall is turned on. To check your firewall, go to Control Panel > System and Security > Windows Firewall - and then select "Check Firewall Status"

Keep your operating system up to date. the best way to do accomplish this is to turn on auto update.

Data Backup

Backup Utility for Windows - This option also come built into the Windows operating system. The utility creates a single backup file of all your data, which you can store on your hard drive, a USB Key, an external hard drive, or burn to a CD or DVD. You can also use the same utility to restore your data from the backup file, should your data become corrupted or lost.

Third Party Backup Software - The best option to backup important files is to use Google Drive. You can save every kind of document here up to 10 GB in size, as well as photos.

Minimize unauthorized access to your accounts and computer

Never share your login ID and/or passwords

Remember you are responsible for any activities associated with your login and password.

Use strong passwords with both upper and lower case characters (e.g., a-z, A-Z) as well as digits and punctuation characters e.g., 0-9, !@#$%^&*(

Passwords should be at least 8 alphanumeric characters.

Passwords should not be a word in any language, slang, dialect, jargon, etc.

Passwords should not be based on personal information, names of family, etc.

Passwords should never be written down or stored online.

How to Protect Your Identity

Critical data must be protected from threats such as unauthorized physical access, theft, or destruction.

Always keep laptops secured, do not leave them in a public place or exposed in a vehicle. Use cable locks if it is exposed to the public eye.

Shred all papers that contain personal/sensitive information that are no longer needed. If they are needed, lock them up.

Do not leave computers logged in if you are away . Always press “Windows key + L” OR “Ctrl +Alt + Delete” and click “Lock Workstation”.

Never permit individuals into access controlled areas without proper identification or authority. Always check if you are suspicious.

Malware

Malware is short for “malicious software." It includes viruses and spyware that get installed on your computer, phone, or mobile device without your consent. These programs can cause your device to crash and can be used to monitor and control your online activity. Criminals use malware to steal personal information, send spam, and commit fraud.

Keep your computer's OS and software current.

Configure your computer to update its operating system automatically and keep applications up to date.

Don't click on any links or open any attachments in emails unless you know who sent it and what it is

Download and install software only from websites you know and trust.

Use a pop-up blocker and don't click on any links within pop-ups.

Run regular virus scans and keep virus software up to date.

How to Protect Your Identity

Critical data must be protected from threats such as unauthorized physical access, theft, or destruction.

Always keep laptops secured, do not leave them in a public place or exposed in a vehicle. Use cable locks if it is exposed to the public eye.

Shred all papers that contain personal/sensitive information that are no longer needed. If they are needed, lock them up.

Do not leave computers logged in if you are away . Always press “Windows key + L” OR “Ctrl +Alt + Delete” and click “Lock Workstation”.

Never permit individuals into access controlled areas without proper identification or authority. Always check if you are suspicious.

Social Engineering/Phishing

Attackers using social engineering techniques often use the telephone to convince network users that they are trusted partners, such as co-workers, information technology staff, or supervisors. These “trusted partners” often gain access to your computer or network by simply asking you for your password to gain access to your confidential data which can then be compromised. When internet fraudsters impersonate a business to trick you into giving out your personal information, it’s called phishing. Don't reply to email, text, or pop-up messages that ask for your personal or financial information. Don’t click on links within them either – even if the message seems to be from an organization you trust. It isn’t. IT Services and legitimate businesses will NEVER ask you to send sensitive information through insecure channels.

Easy Ways to Protect Yourself Online

Protecting yourself while being online is crucial to staying safe and avoiding malicious attacks. Check out our tips below to minimize your risk online.

1. Use Updated Antivirus Software

Antivirus/anti-malware software routinely scans your device for indications of known computer viruses and malware. While these programs cannot prevent everything from affecting your computer, installing a reliable antivirus software package and keeping its definitions up-to-date can save you from potential headaches that come with being infected.

Find out more about Antivirus below in the Sophos Antivirus section below.

2. Use an Updated Operating System

Ensure the Automatic Updates and the Firewall are ON for your operating system. Make sure to also keep applications such as flash, java, chrome etc. up to date as well.

3. Keep Your Browser Up to Date

Using updated Browsers will help ensure the best security while browsing many sites. Updated browsers will often scan sites and alert you as to whether they are safe to go to when clicking on links.

For tips on how to keep you Mozilla Firefox up-to-date click here

For tips on how to keep your Google Chrome up-to-date click here

For tips on how to keep your Apple Safari up-to-date click here

4. Know The Source

Whether you're surfing the Internet, checking your email, responding to IM or file sharing– Don't click on anything unless you asked someone to send it to you. Links, attachments, and files can contain malicious code, and clicking on them gives way for that code to execute. When in doubt, go directly to the source! Never follow an email link to a banking, credit card, or merchant site. Always type the known address into your browser.

5. Use Secure Passcodes

Whether it is a passcode to your device, email, social media platform or bank account, keep it secure by making it at least 8 characters in length (12 or more is preferred), using a combination of characters (numbers, upper and lowercase letters and symbols) and avoiding using common words (names, places, dictionary words). RMU provides guidance and tips on passwords through the LevelUp program.

Find out more about LevelUp @ https://rmu.edu/levelup

6. Don't share illegal files

Uploading and downloading music, movie, and software files that are copyright protected is illegal without proper licensing. Also, the P2P networks that are used to trade files are becoming the preferred method to spread malware & viruses.

Identity Theft Protection

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security, credit card or driver's license numbers, in order to impersonate someone else often for financial gain. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

What can I do?

1. Do not give out personal information over the phone, through the mail or over the Internet, unless you have initiated the contact or are sure that you know who you are dealing with.
2. Guard your physical mail and trash from theft, use a paper shredder for any personal information.
3. Before revealing any personal identifying information, find out how it will be used, secured, and whether it will be shared with others.
4. Ask if you have a choice about the use of your information.

5. Do not carry your Social Security card; leave it in a secure place.
6. Give your SSN out only when absolutely necessary.
7. Pay attention to billing cycles. If you do not receive your bills on time, follow up with the creditor. A missing credit card bill could mean an identity thief has taken over your account and changed your billing address to cover his/her tracks.
8. Be wary of promotional scams which occur over the phone, online and through the mail.
9. Place a fraud alert on your credit report from each of the three major credit bureaus if you suspect anything.
10. Only conduct online shopping with known and reputable organizations. Never follow links in an email and provide personal information always go directly to the known website and ensure it is being used over a secure connection (SSL- ensure lock is at the bottom of window.)

If you think you are a victim of Identity theft take the following actions:

Close accounts and cancel credit cards where suspicious activity occurred

File a Police Report

File a complaint with the Federal Trade Commission

Contact the fraud department at each of the three major credit bureaus:

Equifax: https://www.equifax.com

Experian: https://www.experian.com

TransUnion: https://www.transunion.com

For check fraud contact the three major check verification companies

TeleCheck: 800-710-9898

Certegy: 800-437-512

Mobile Security

With over 5.3 billion mobile phone subscribers worldwide, these mobile devices are now conventional gadgets for data storage and communication. But, compared to PCs, mobile devices and other mobile devices are more prone to be lost or stolen. This causes a huge risk of identity theft, compromised information, and financial loss. Below is a list of some basic steps you can take to protect yourself and your data.

Basic Tips to Protect Your Mobile Devices

• **Enable Auto Lock:** Whether you are using an iPhone, iPad or an Android based mobile devices, make sure you have enabled the built-in phone lock feature with a strong password. This adds an extra layer of security to your mobile device and prevents unauthorized access; even it is lost or stolen.

• **Update Your Device:** Be sure to always update your device when prompted or when update is available. These updates include fixes for bugs, vulnerabilities, and additional features. This will ensure your device is protected against the latest security risks. NEVER put off an update, as this greatly increases your chances of a security breach.

• **Backup Your Mobile Devices's Data:** The biggest risk of losing a mobile device is perhaps letting all your important data go into wrong hands. The wisest thing you could do is to have backup of all your important data – phonebook, photos, messages etc…The backed up data can later be used for restoration on your new mobile devices.

• **Lock Sensitive Applications:** Another useful way to protect your personal data on your mobile devices is to make use of an application locker utility. Having your mobile devices configured with this utility will prevent unauthorized access to applications that contain sensitive personal information, such as Messaging, Phonebook, Gallery, etc… Even if someone finds or steals your phone, they cannot access these protected apps without a valid password.

• **Proper Disposal:** When you are getting ready upgrade to a new device, be sure to perform a factory reset. This will ensure your device is clean of any personal data;

including account passwords, email, photos, ect. If your upgrading your mobile device, remember to remove or format your SD card.

Sophos Antivirus

Antivirus/anti-malware software routinely scans your device for indications of known computer viruses and malware. While these programs cannot prevent everything from affecting your computer, installing a reliable antivirus software package and keeping its definitions up-to-date can save you from potential headaches that come with being infected. RMU recommends Sophos Home for faculty, staff and students.

Resident students are required to have active anti-virus software running on devices connected to the network.

Sophos Home

How to Encrypt Files with AES-256

-

Encrypting Files with 7-zip

7-Zip is an open source software used to compress or zip files secured with encryption. When you send or transfer files that contain Personal Identifiable Information (PII) or other
confidential and sensitive data, the files must be encrypted to ensure they are protected from
unauthorized disclosure.

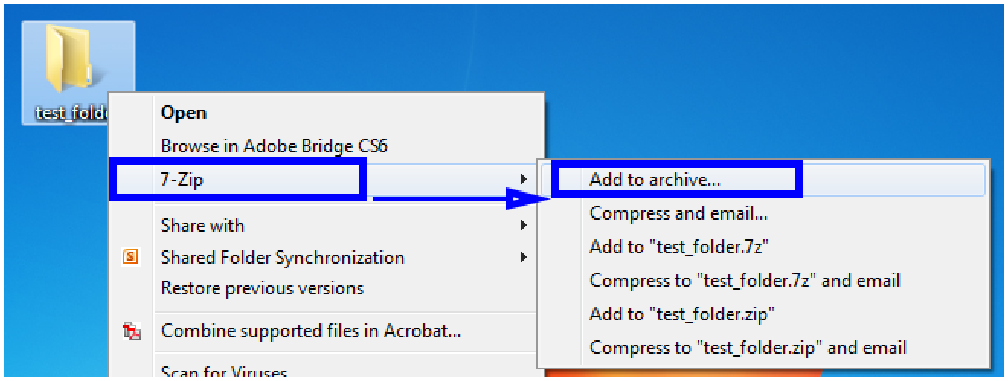
For Mac OS instructions, please visit: https://osxdaily.com/2012/01/07/set-zip-password-mac-os-x

7-Zip, like WinZip, creates a container called archive that holds the files to be protected. That archive can be encrypted and protected with a password. 7-Zip is a free software that creates Zip files that can be opened with WinZip or other similar programs.

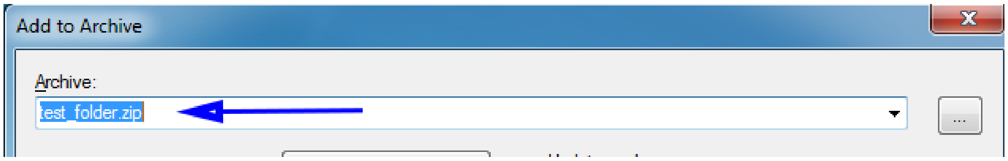
To obtain a copy of 7-Zip, please see https://www.7-zip.org and select the Download link. Once the software is installed, please follow these steps to encrypt a file or folder.

Step 1: Right click on the file / folder to be encrypted.

Step 2: Select “7-Zip” then “Add to archive…”

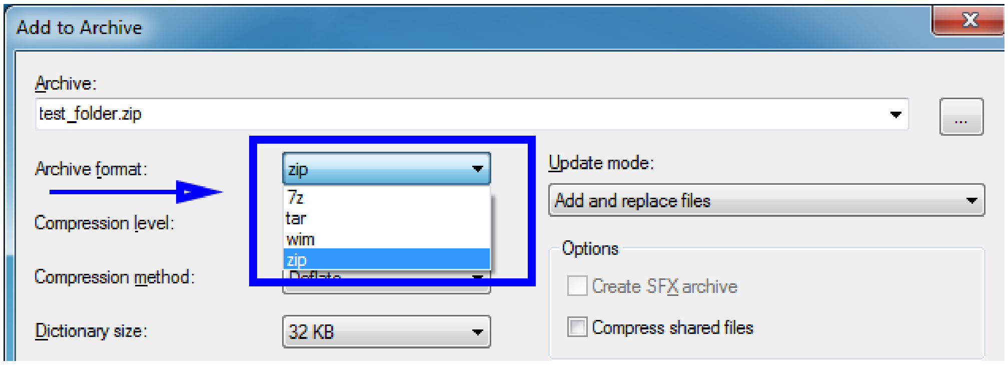

test_fold
Open
Browse in Adobe Bridge CS6
7-Zip
Share with
Shared Folder Synchronization
Restore previous versions
Combine supported files in Acrobat...
Scan for Viruses
Add to archive...
Compress and email...
Add to "test_folder.7z"
Compress to "test_folder.7z" and email
Add to "test_folder.zip"
Compress to "test_folder.zip" and email

Step 3: In the Add to Archive window change the name of the archive you wish to create.



Archive: test_folder.zip

Step 4: Change the Archive Format to "Zip".



Archive: test_folder.zip

Archive format: zip

Compression level:

Compression method: Deflate

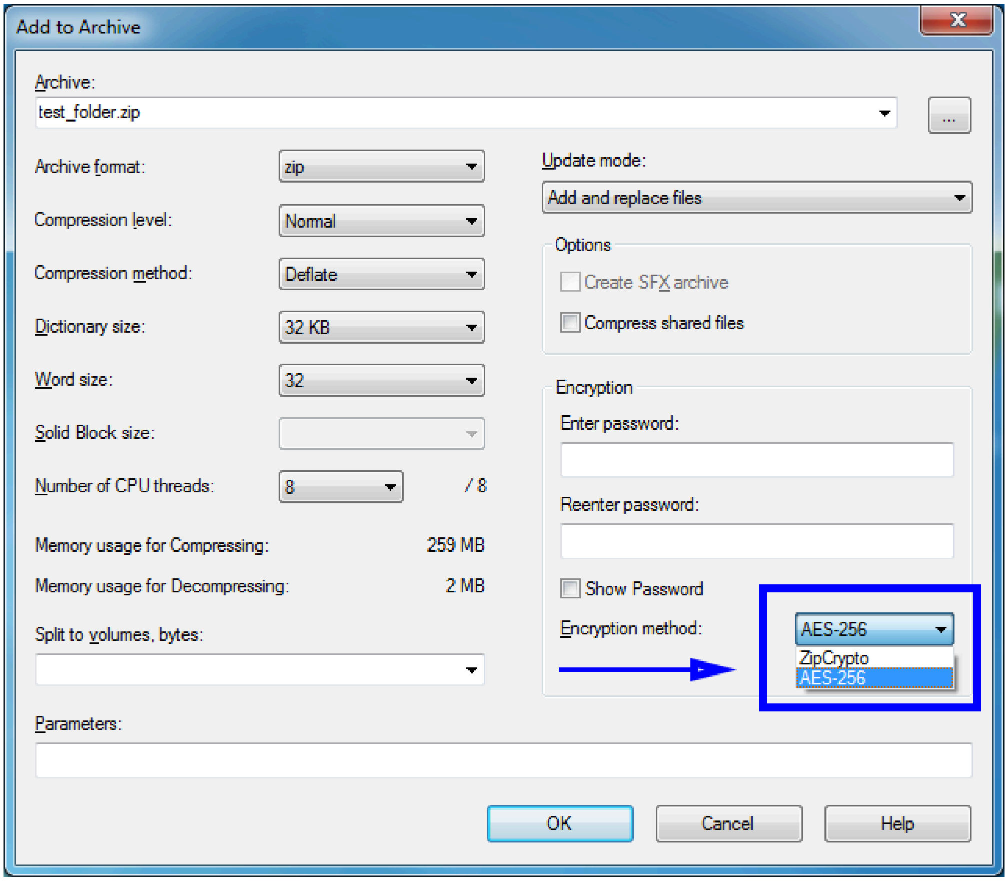
Dictionary size: 32 KB

Update mode: Add and replace files

□ Create SFX archive

□ Compress shared files

Step 5: Change the Encryption Method to “AES-256”. There is a trade-off between using AES-256 and ZipCrypto. AES-256 is proven much more secure than ZipCrypto, but if you select AES-256 the recipient of the zip file may have to install 7-zip or another zip program to read the file contents. Selecting ZipCrypto may allow users to open the zip file in Windows without a zip program, but it does not provide adequate protection against attackers with modern cracking tools. It is strongly recommended to use AES-256 to protect sensitive and confidential data.



Archive: test_folder.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 8 / 8

Memory usage for Compressing: 259 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

□ Create SFX archive

□ Compress shared files

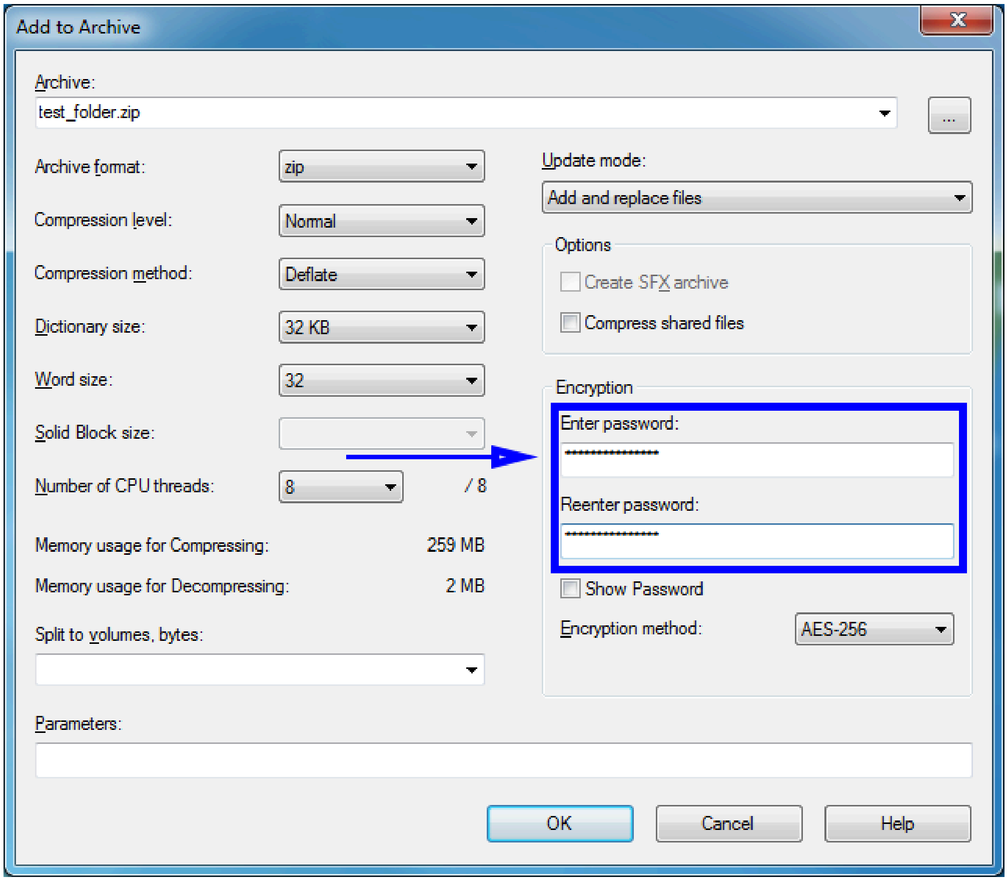
Enter password:

Reenter password:

□ Show Password

Encryption method: AES-256

Step 6: Enter a Password. Use a strong password with at least 8 characters containing upper and lowercase letters, and a minimum of one number.



Archive: test_folder.zip

Archive format: zip

Compression level: Normal

Compression method: Deflate

Dictionary size: 32 KB

Word size: 32

Solid Block size:

Number of CPU threads: 8 / 8

Memory usage for Compressing: 259 MB

Memory usage for Decompressing: 2 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Options

□ Create SFX archive

□ Compress shared files

Encryption

Enter password: ****************

Reenter password: ****************

□ Show Password

Encryption method: AES-256

Step 7: Select “Ok” to create the encrypted archive file. The new archive file will be located in the same folder as the original. Best security practices recommend that you do not email the password with the Zip file as it could be intercepted in transit. It is better to call the recipient of the Zip file and convey the password over the phone.

Robert Morris University - Pittsburgh
6001 University Blvd., Moon Township, PA 15108
412-397-3000

Contact RMU

Accreditations

Privacy Policy

Ethics Policy

Book Store

Disclosures

U-Can

Title IX

Academic Accommodations / Services for Students with Disabilities

GIVE | VISIT | GET INFO | APPLY

Password Help

Robert Morris University | Pittsburgh, PA

Have you forgotten your password or need assistance in resetting your existing password? Please review the instructions below and if additional assistance is needed, please contact the IT Help Desk.

Expired / Forgotten / Resetting Passwords

If you have forgotten your password or if it has expired, you can reset it by visiting rmu.edu/password.

In order to reset your password, you will need to provide your RMU ID card number, last four digits of your social security number, along with your date of birth (to validate your identity).

New User Account Activation

Please visit: rmu.edu/activate

You will need to provide your RMU ID card number, last four digits of your social security number, along with your date of birth (to validate your identity).

Password Requirements

> Password Length: Passwords must be a minimum of 10 characters
>
> Complexity Requirements: Passwords must contain characters from three of the following:

Uppercase letter (A-Z)

Lowercase letter (a-z)

At least one numeric digit (0-9)

At least one special character (~ ! # % ^ * - + = ( ) { } [ ] : . ? /)

Password must not contain any part of your user name, be easily guessable, or have been previously known to be compromised.

Password Expiration: Passwords will expire after one year.

Password History: Previously used passwords will not be allowed.

Contact | Campus Map

Robert Morris University - Pittsburgh
6001 University Blvd., Moon Township, PA 15108
412-397-3000

Contact RMU

Book Store

Accreditations

Disclosures

Privacy Policy

U-Can

Ethics Policy Title IX

Academic Accommodations / Services for Students with Disabilities