Sending sensitive data by email using Outlook

Sensitive Data transmission using Outlook

Purpose

This document provides operating instructions for using cryptographic controls to protect sensitive data. Sensitive data must be protected from exposure to unauthorized persons or when it is exchanged with authorized recipients outside the normal security boundaries of the VCCS network. Authorized recipients may include other VCCS employees, consultants, cloud services providers, or other entities with approved non-disclosure and acceptable use agreements on file.

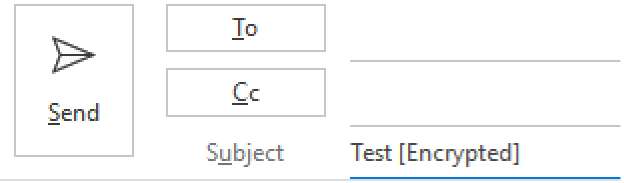
Transmitting Sensitive Data Using Email

Transmission of sensitive data using email is not allowed unless the data is included as an encrypted attachment or the email itself sent encrypted. Note that some email servers will reject or strip off unrecognized attachments, so this method is not always reliable. One method is to send the encryption key (password) to the recipient using an alternate communication method (e.g. cell phone) to ensure the data and the encryption key are transmitted separately.

1. Use built-in encryption in Office365 Outlook

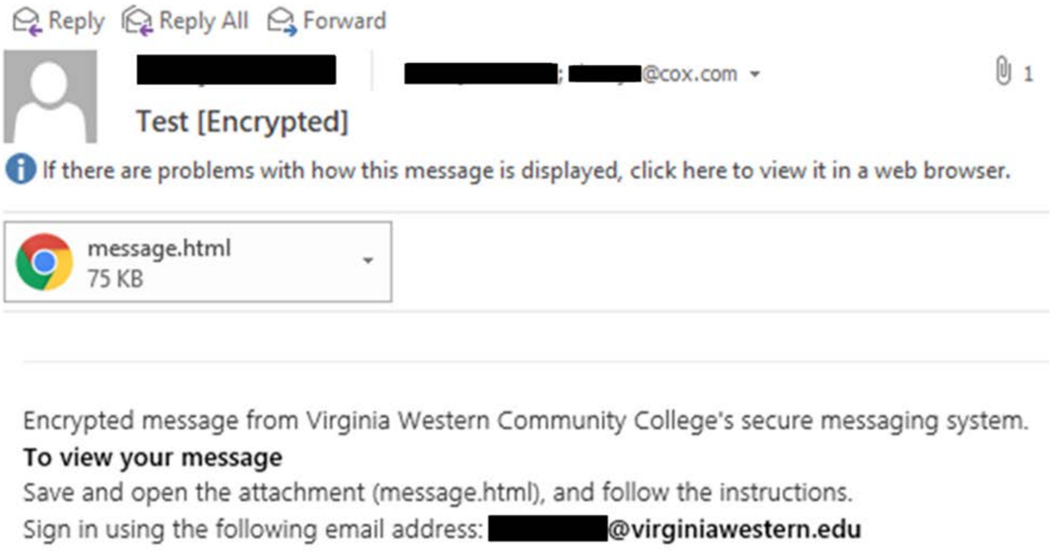
VWCC uses built-in encryption in Outlook.

- Include the text **[Encrypted]** in the subject of the email



Subject: Test [Encrypted]

- If the recipient is also a Microsoft Outlook user, they will see something like this:



[redacted] [redacted]; [redacted]@cox.com

Test [Encrypted]

If there are problems with how this message is displayed, click here to view it in a web browser.

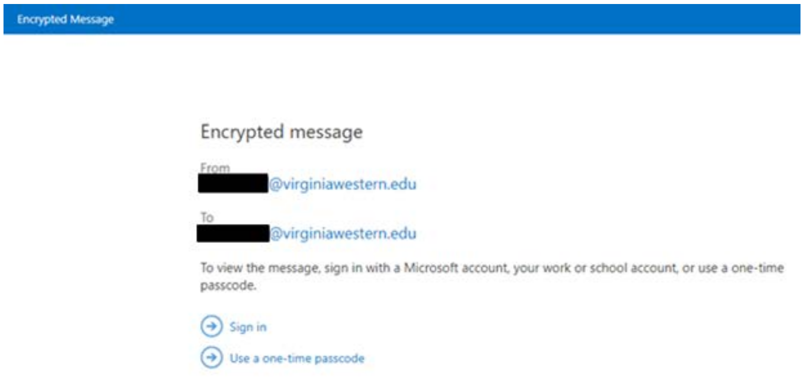
Encrypted message from Virginia Western Community College's secure messaging system.

To view your message

Save and open the attachment (message.html), and follow the instructions.

Sign in using the following email address: [redacted]**@virginiawestern.edu**

- Clicking on _message.html_ will open the browser window below:



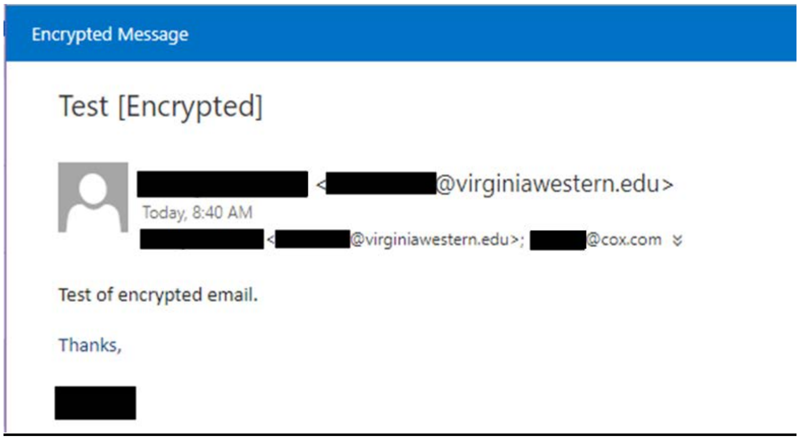
Encrypted message

From
[redacted]@virginiawestern.edu

To
[redacted]@virginiawestern.edu

To view the message, sign in with a Microsoft account, your work or school account, or use a one-time passcode.

- Once they sign in, they will be able to view the decrypted message.



Test [Encrypted]

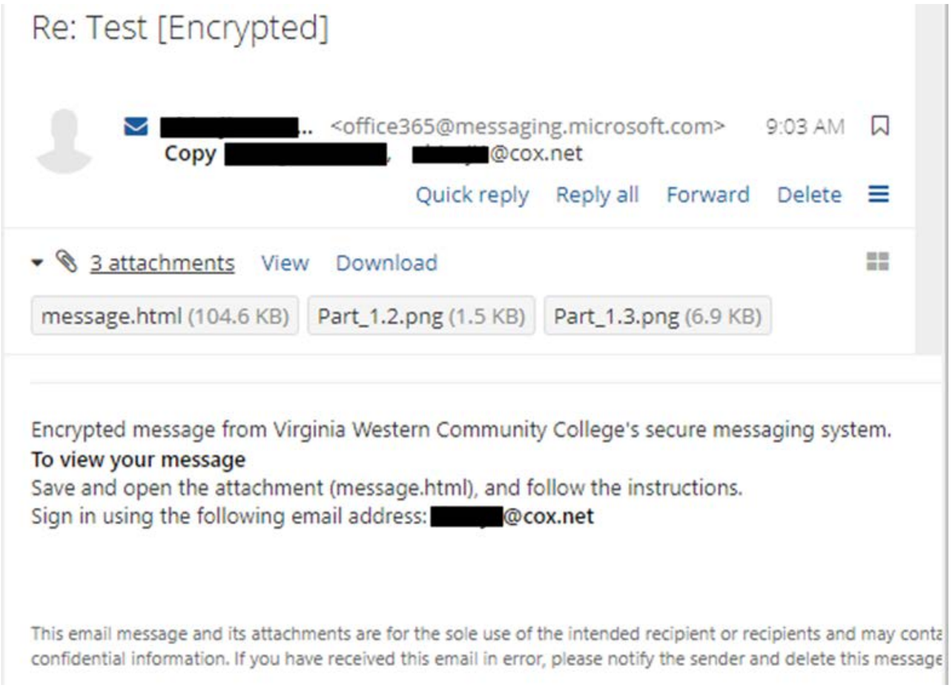
[redacted] <[redacted]@virginiawestern.edu>
Today, 8:40 AM
[redacted] <[redacted]@virginiawestern.edu>; [redacted]@cox.com

Test of encrypted email.

Thanks,

[redacted]

- External email users (like Gmail etc.) get a similar email asking them to sign in.



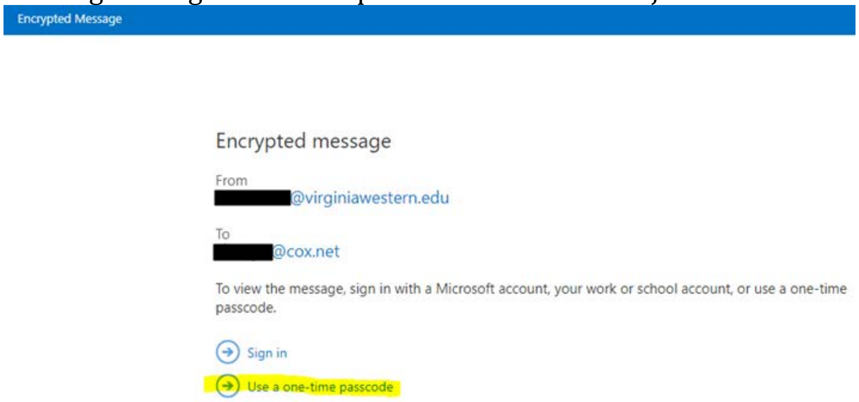
Re: Test [Encrypted]

[redacted].. <office365@messaging.microsoft.com> 9:03 AM
Copy [redacted], [redacted]@cox.net

Encrypted message from Virginia Western Community College's secure messaging system.
To view your message
Save and open the attachment (message.html), and follow the instructions.
Sign in using the following email address: [redacted]**@cox.net**

This email message and its attachments are for the sole use of the intended recipient or recipients and may conta
confidential information. If you have received this email in error, please notify the sender and delete this message

- Clicking message.html will open a browser window just like the one for Outlook



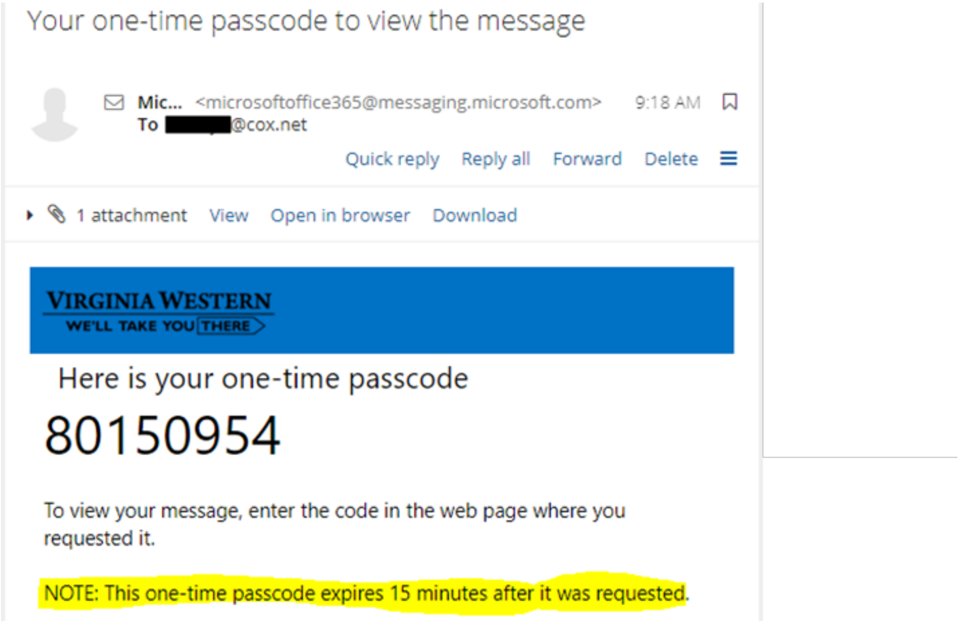
Encrypted message

From
[redacted]@virginiawestern.edu

To
[redacted]@cox.net

To view the message, sign in with a Microsoft account, your work or school account, or use a one-time passcode.

- Since they aren't Outlook users, they will need to sign in using a one-time passcode sent to their email,


Your one-time passcode to view the message

Mic... <microsoftoffice365@messaging.microsoft.com> 9:18 AM
To [redacted]@cox.net

Here is your one-time passcode

80150954

To view your message, enter the code in the web page where you requested it.

NOTE: This one-time passcode expires 15 minutes after it was requested.

after which they will be able to view the email.

2. Secure a copy of the original source data

Encryption of original source data, original data sets, original documents, or original files containing sensitive data is not permissible unless the encryption keys are managed within an approved central encryption key repository. Copies may be encrypted and transmitted using email *only* when the encryption key can be sent to the recipient of the data by an alternative method or by using the built-in encryption in Office 365 Outlook described above.

- Microsoft Office documents must be encrypted using the password protection functionality built into the Microsoft Office 2013 and later version products using strong encryption (128-bit AES) with a SHA-2 class-hashing algorithm. Earlier versions of Microsoft Office products are not permissible for encryption purposes.
- Adobe Acrobat Professional X and later versions (we have version 17), conform to the 128-bit AES encryption specification and can encrypt PDF format documents using the built-in password protection functionality as an acceptable alternative to Microsoft Office.
- Convert other document or file types to a supported Microsoft Office365, Adobe Acrobat Professional, or more recent version of these products and then apply password encryption.

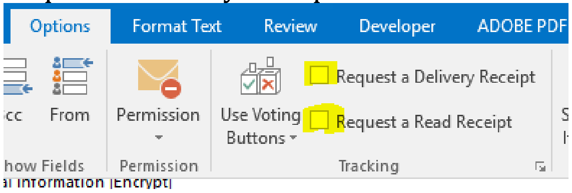
3. Attach the encrypted file to your email message

Using your VCCS email account, attach the encrypted file to the message and notify the recipient that the attachment is encrypted

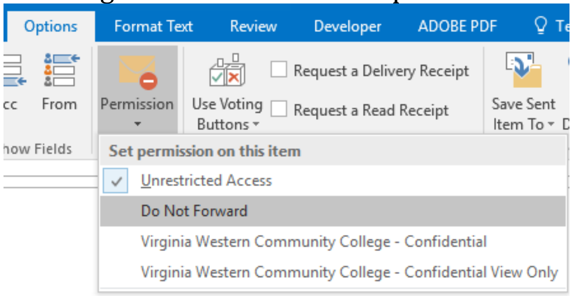
- Contact the recipient by telephone or by text message to convey the password used to decrypt the encrypted data file if using password-protected encryption.
- Do not send the password by email to the recipient.

4. Request the recipient to acknowledge receipt of your email message

Request a Delivery Receipt as well as a Read Receipt for your message.



If using Microsoft Outlook, you can also set Permission on the message to restrict forwarding by selecting the Do Not Forward option under the Options Tab.

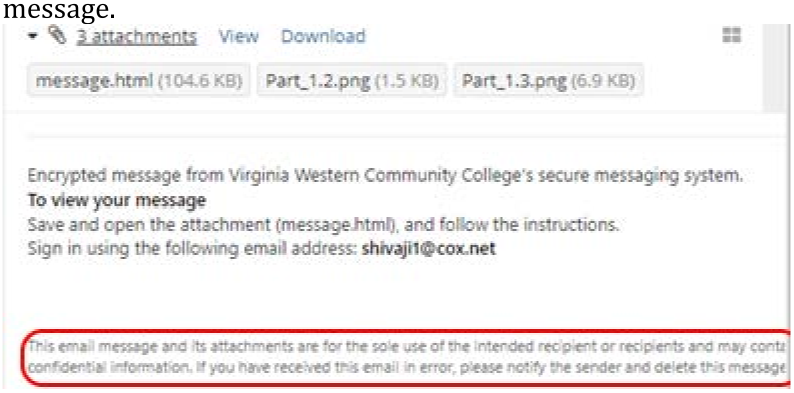


- The recipient will receive an email message prompting them to logon using their Microsoft Account or by using a one-time passcode like in Office365 encryption described in **Step 1**.
- The recipient can download the attachment but will not be able to forward the attachment automatically to another email address.

5. Archive or delete the encrypted file

Unless there is a demonstrated need to retain a copy of the data set in encrypted format, any copy of the original data and encrypted versions must be deleted. Only original source data is to be retained per Library of Virginia data retention requirements.

- Any transmission of VCCS sensitive data must include a statement indicating the recipient is authorized to use the data for its intended purpose only and that the recipient must delete or return any VCCS sensitive data as directed when the data is no longer required. Note that the Office365 built-in encryption process described in Step 1 automatically includes this message.



Encrypted message from Virginia Western Community College's secure messaging system.

To view your message

Save and open the attachment (message.html), and follow the instructions.

Sign in using the following email address: **shivaji1@cox.net**

This email message and its attachments are for the sole use of the intended recipient or recipients and may conta confidential information. If you have received this email in error, please notify the sender and delete this message

SUMMARY

To summarize:

- The easiest way to send sensitive data via email is to use the built-in encryption mechanisms outlined in Item 1.
- For document attachments, further security is afforded by encryption of the documents (using the methods supported by software used to create the document) as described in Items 2-3 and sending the associated password/encryption key to the recipient using an alternate method of communication like a phone or voice message.
- Items 4-5 list best practices for dealing with the sensitive data after transmission.