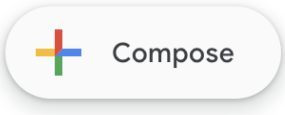
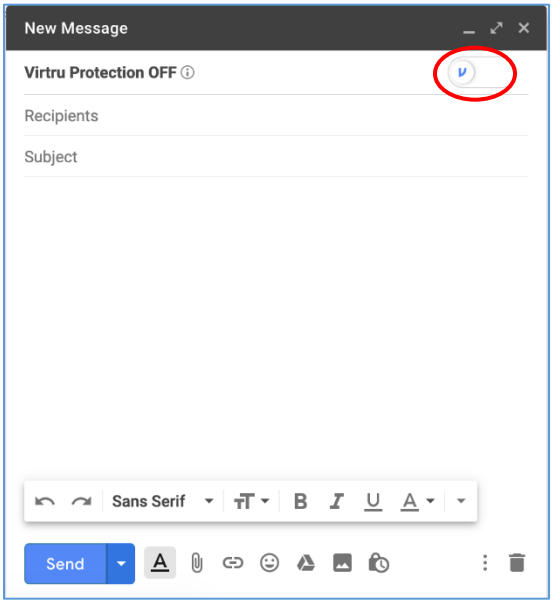
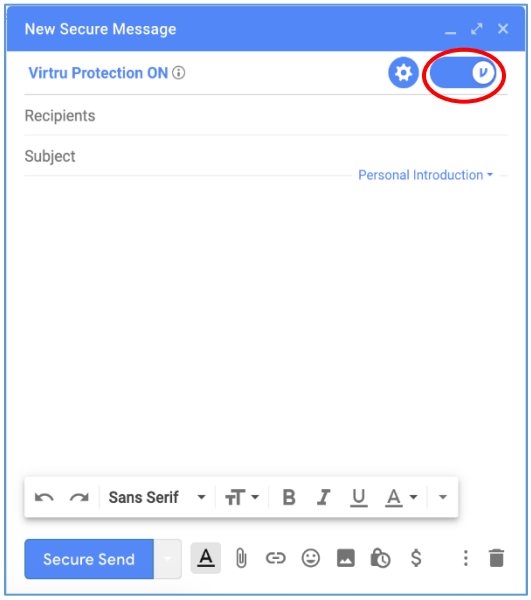
Steps to Encrypt

1. In Gmail, click *Compose*.

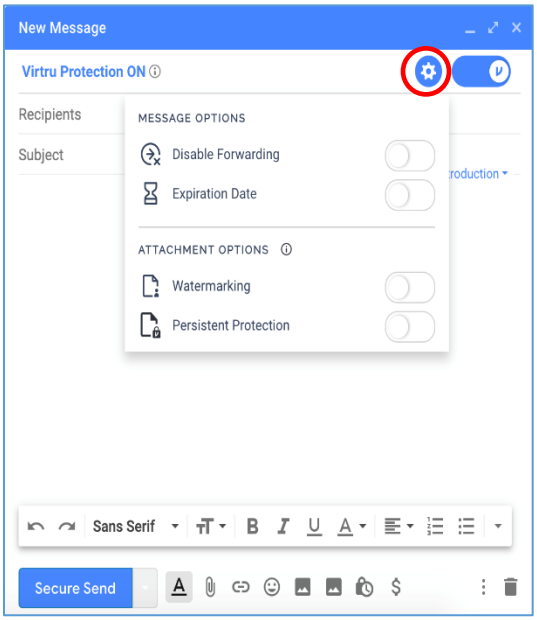


2. You should see the Virtru bar at the top of the *Compose* window. If it is *OFF*, click the toggle to turn it *ON.*

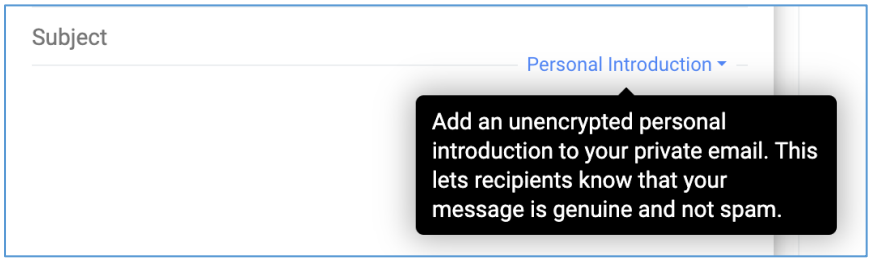




3. Add your recipients, subject, body of the email, and any relevant attachments. If you wish, you can select the *gear* icon to set additional *Security Options* for the message, including Disable Forwarding, setting an Expiration Date, and applying Watermarking and/or Persistent File Protection (PFP) to attachments.



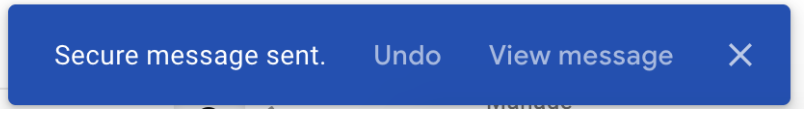
You can also set a one-time, unencrypted personal introduction for the message to either introduce Virtru to new users or provide some context about the email. Just click *Personal Introduction* in your draft window and enter any content you wish to be delivered unencrypted.



Note: Special formatting not supported. The Personal Introduction only supports plain text and line breaks.

4. Once your message is ready and applicable settings are in place, just click *Secure Send*.

You will see a brief animation, then the message will encrypt and send!

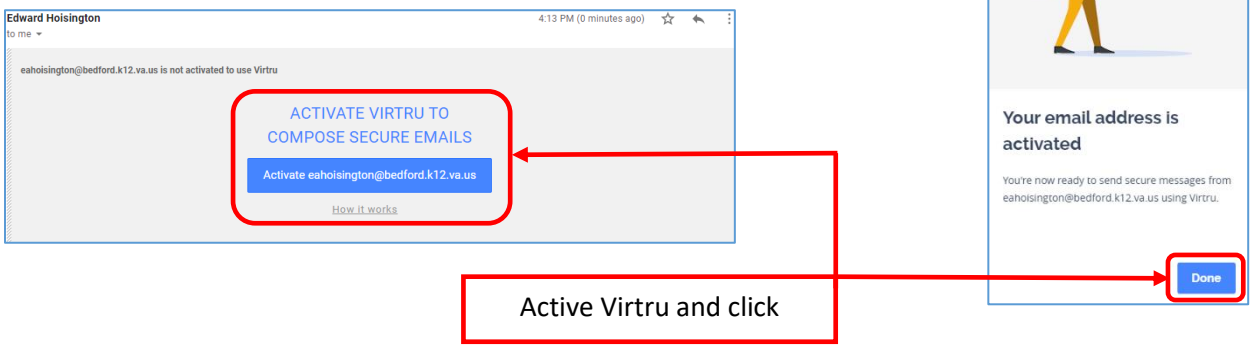


If your recipients have Virtru, the message will decrypt in their mailbox. If they are not Virtru users, they can access the message in our Secure Reader.

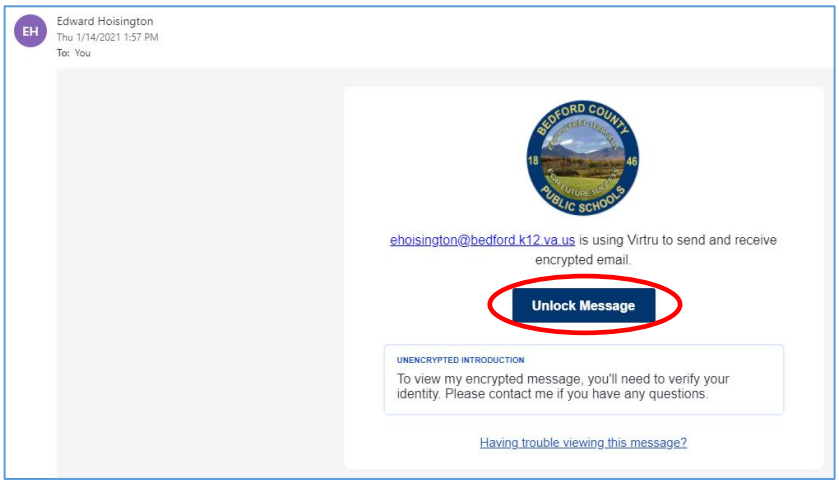
Recipient Experience

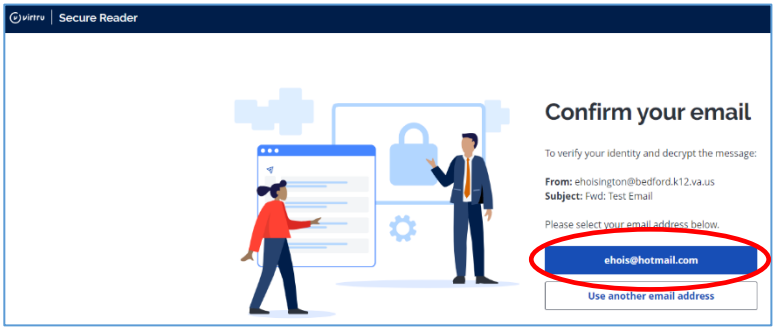
Recipients with Virtru will receive the message already decrypted.

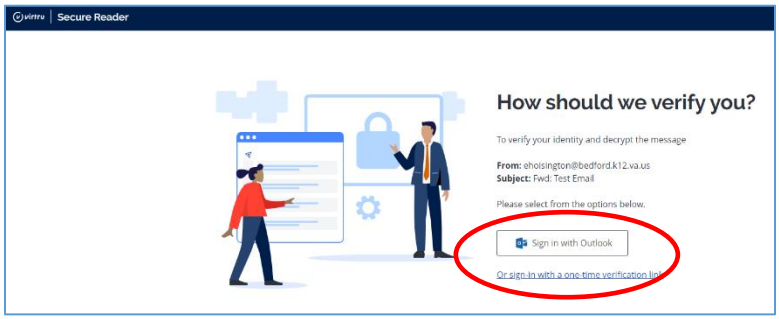
Recipients with the Virtru extension but are not Virtru users. Activate Virtru by click on the *Activate youraddress@email.com* button. Click *Done* on the next message box.



Recipients without Virtru extension and not Virtru users. Users will need to click on the *Unlock Message* button and confirm your email on the next message box. On the *How should we verify you?* screen, choose how you will verify you email – sign in through Google, Outlook, or sign-in with a one-time verification link.







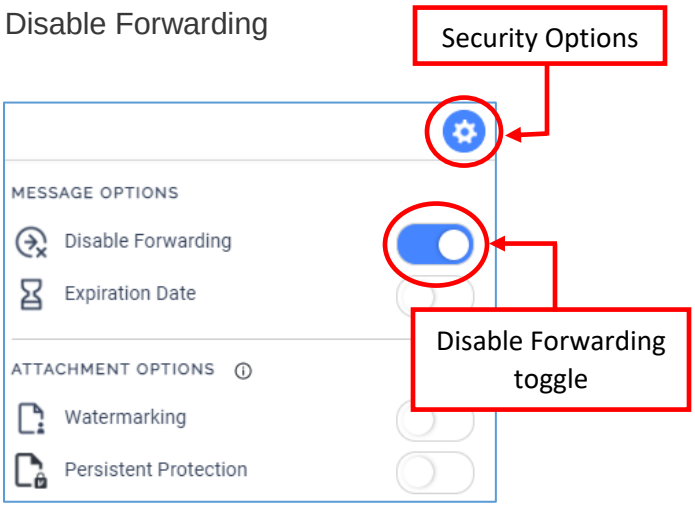
Manage Disable Forwarding in Virtru Email

Disable Forwarding can be set before an email is sent

Disable Forwarding: This setting makes your message your message unreadable if it's been forwarded.

The following steps demonstrate how to apply the Disable Forwarding Security Option while composing an email:

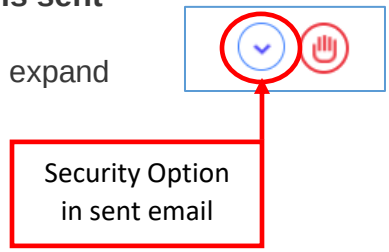
1. Open a new draft and toggle Virtru *ON*.
2. Open the *Security Options/Settings* menu. Select *Disable Forwarding* from the menu.



3. Compose the rest of your message and *Send*.

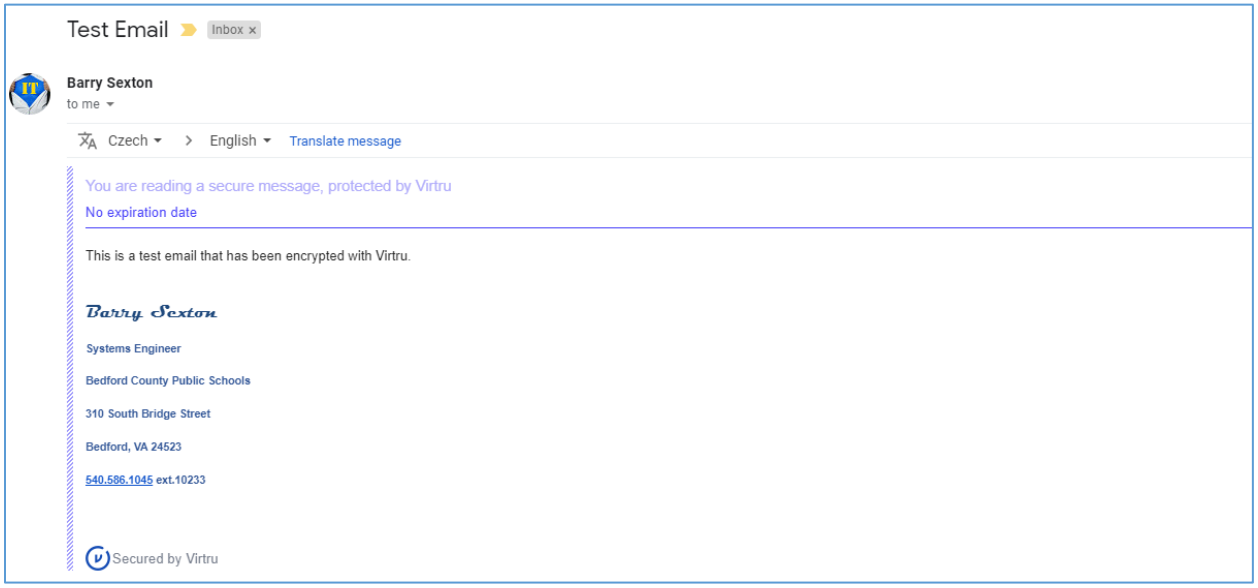
Disable Forwarding can also be managed after an email is sent

1. With Virtru enabled, open the sent secure message and expand the *Security Options/Settings* menu.
2. Select or deselect the *Disable Forwarding* option.

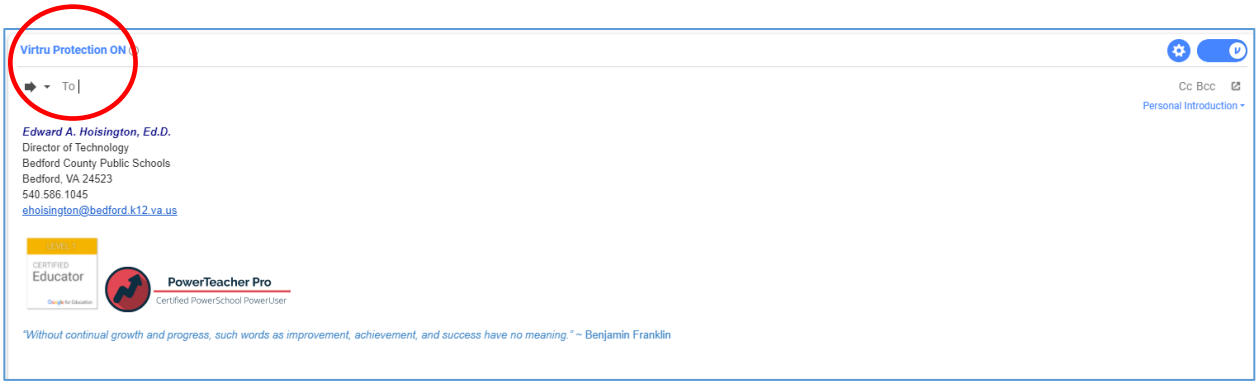


Recipient Experience

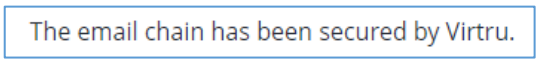
When the intended recipient receives the message, they will be able to decrypt the message like any other email secured by Virtru.



If the recipient attempts to forward the message, it will appear to send as any other forwarded email. If the recipient has Virtru, the message will remain protected.



However, when the secondary recipient receives the forwarded message, they will only have access to the most recent entry in the thread. The following message will be displayed.



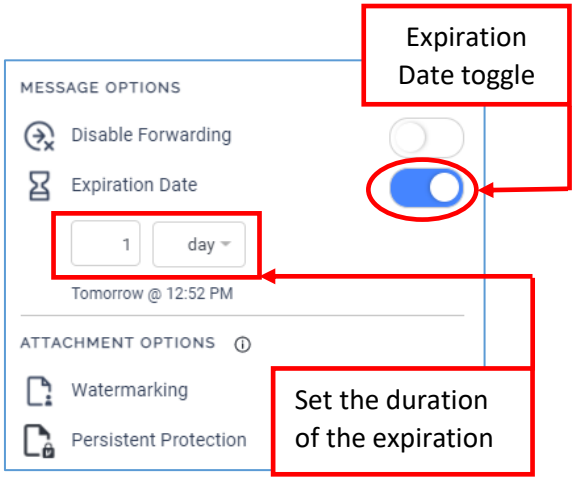
Recipients with Virtru will have the *Show last secure message* button with dropdown, they can click on this button to see the next threaded message.

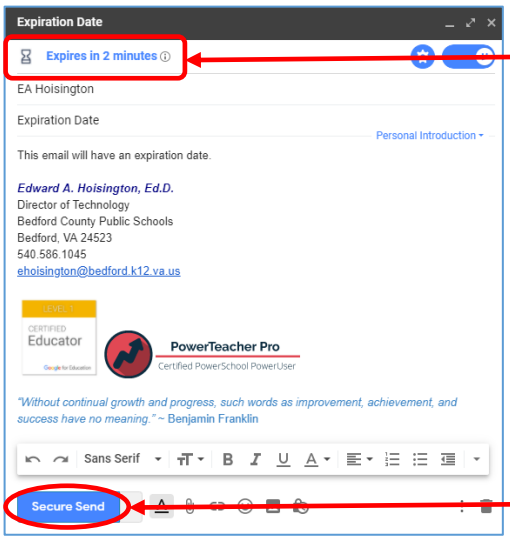
Manage an Expiration Date in Virtru Email

An expiration can be set before an email is sent

Expiration Date: Set a specified time your recipients will no longer have access to the email message.

1. Open a new draft and toggle Virtru *ON*.
2. Open the *Security Options/Settings* menu.
3. Select *Expiration Date* from the menu and configure the deadline.
    a. Set the number of…
    b. Minutes, Hours, Days, Weeks, Months, and Years
4. Compose the rest of your message and *Send*.





Duration of the expiration displayed on email prior to Secure Send

Click the Secure Send button once expiration date duration is

Expirations can also be managed after an email has been sent

1. With Virtru enabled, open the sent secure message and expand the *Security Options/Settings* menu.

2. Select *Expiration Date* and modify accordingly.

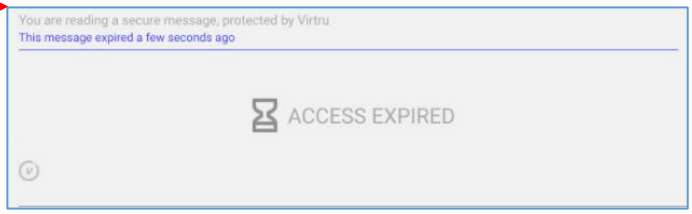
Recipient Experience

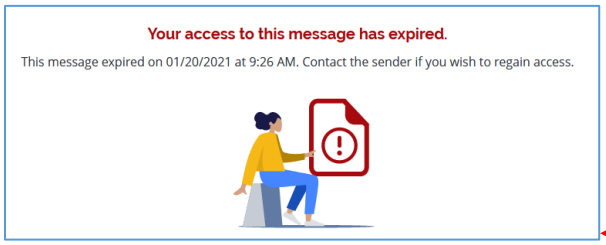
Expired Email

When the intended recipient receives the message before expiration, they will be able to decrypt the message like any other email secured by Virtru.

If the recipient attempts to open the message after expiration, they will receive a prompt indicating their access is expired. This message is consistent whether within Gmail or the Virtru Secure Reader.

Expiration message within Gmail





Expiration message within Virtru Secure Reader

Manage Watermarking in Virtru Email

Watermarking can be set for attachments before an email is sent

Watermarking: Supported attachments (.docx, .pptx, .xlsx, .jpeg, .png, .pdf) will be watermarked in Secure Reader. If a Virtru recipient receives an encrypted file, they can preview the file in the Secure Reader and download a decrypted copy locally. When Watermarking is applied to a secure file, recipients will only have access in the Secure Reader and will see their email address watermarked across the document.

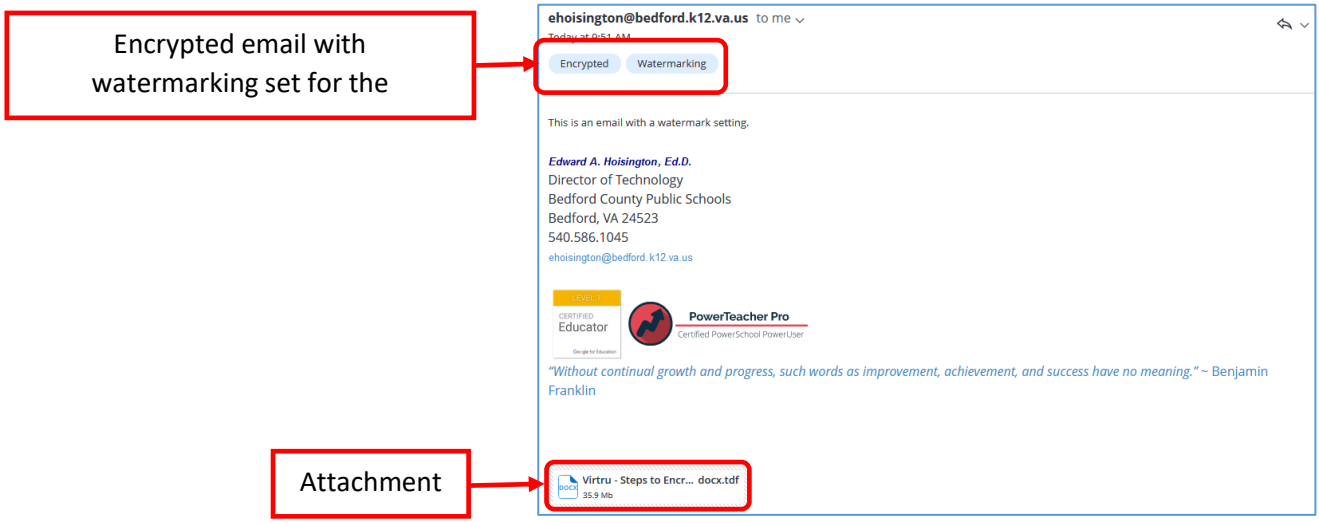
1. Open a new draft and toggle Virtru *ON*.
2. Open the *Security Options* menu.
3. Select *Watermarking* from the menu.
4. Compose the rest of your message and *Send*.

Watermarking can also be managed after an email is sent

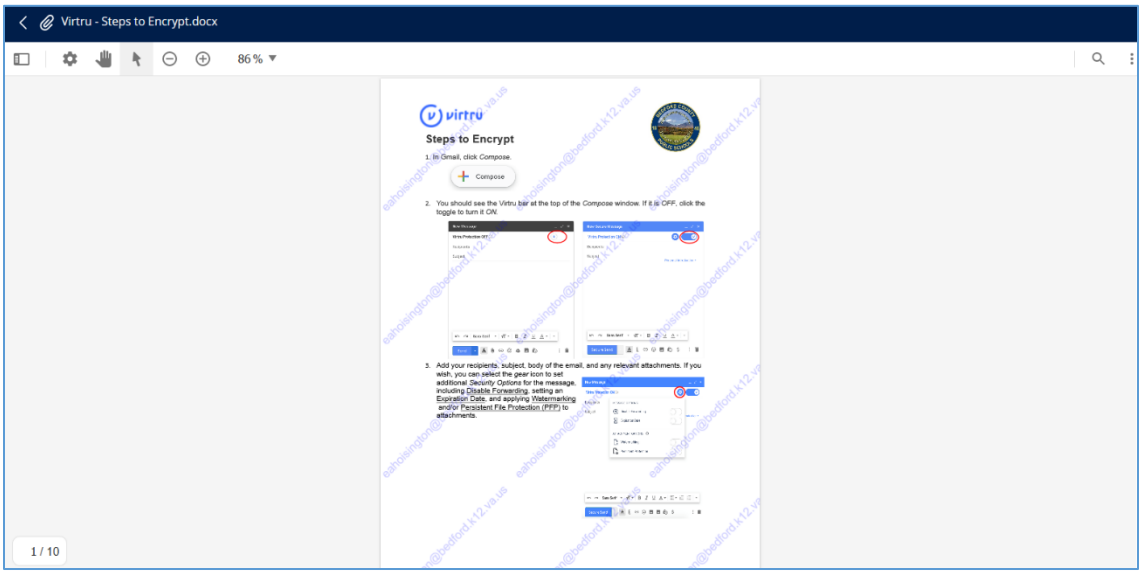
1. With Virtru enabled, open the sent secure message and expand the *Security Options* menu.
2. Select or deselect the *Watermarking* option.

Recipient Experience

When a recipient receives a watermarked document, even if they are a Virtru plugin user, they will need to view the file in the Virtru Secure Reader:



While viewing, the recipient's email address will be overlaid in a repeating pattern over the opened file and the recipient will not have the option to download the file.



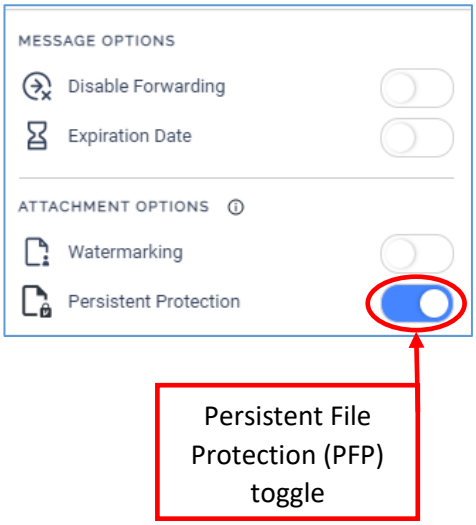
Manage PFP in Virtru Email

PFP can be set for attachments before an email is sent

Virtru users have the ability to apply additional security settings to protected content. Among these settings is the option to apply *Persistent File Protection* (PFP) to an encrypted file.

PFP provides a secure file container that is portable, universally accessible, and built on top of open standards. Regardless of where files are stored, PFP allows you to select, protect, and share a file with anyone while maintaining full visibility into how it is being used and retaining the ability to revoke access at any time. Any file protected with PFP with convert into the .tdf.html file format. This ensures that the contents are only accessible in Virtru's Secure Reader and only authorized parties can view it.

1. Open a new draft and toggle Virtru *ON*.
2. Open the *Security Options* menu.
3. Select *Persistent File Protection/PFP* from the menu.
4. Compose the rest of your message and *Send*.



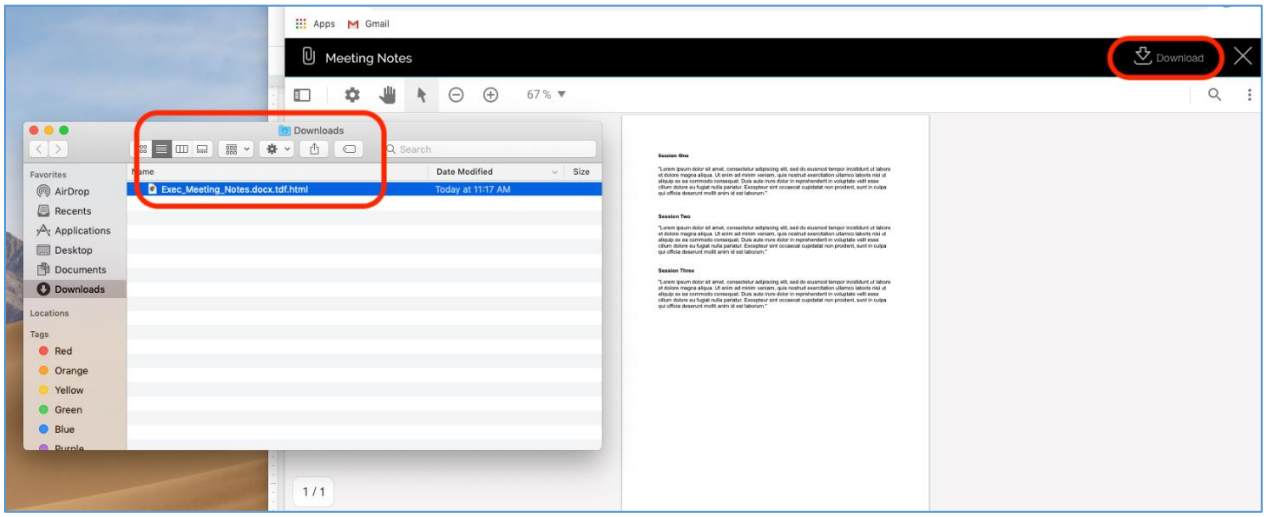
Note: Although newer Microsoft office file types are supported, older versions (*.doc, .ppt, .xls*) are not compatible. Additionally, these other common file types are NOT supported: *.msg, .zip, .md*. with Watermarking and PFP.

PFP can also be managed after an email is sent

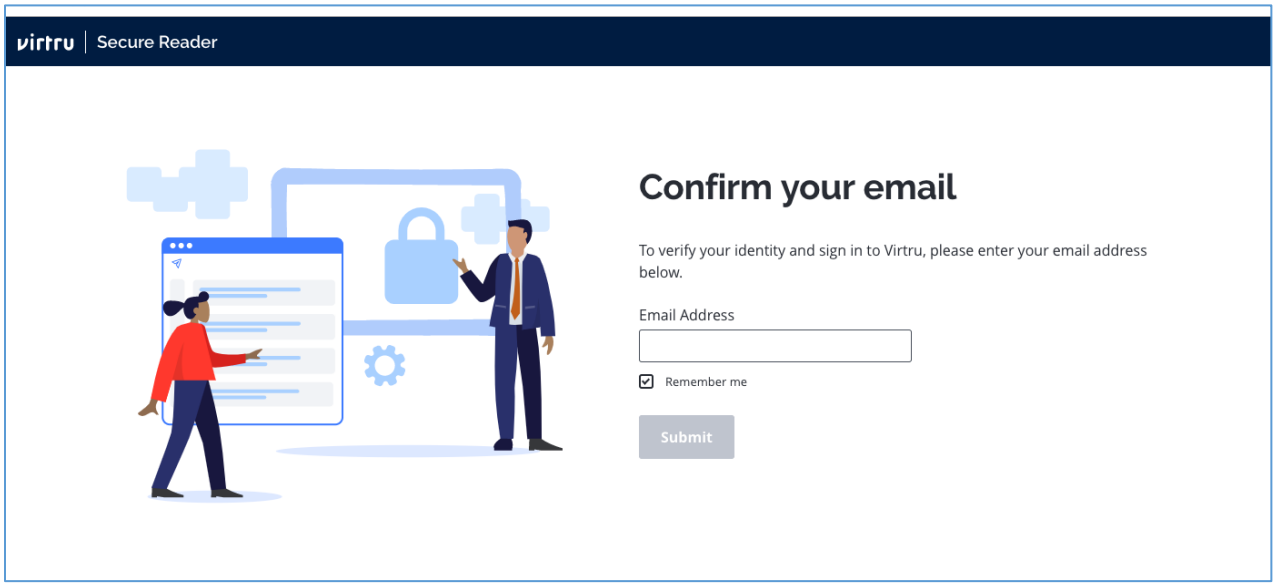
1. With Virtru enabled, open the sent secure message and expand the *Security Options* menu.
2. Select or deselect the *Persistent File Protection* option.

Recipient Experience

When recipients receive an email with a .tdf.html file they will need to view the file in Virtru's Secure Reader. Once the file is unlocked in the Secure Reader, they will have the option to download the file. If downloaded, the file will remain in the .tdf.html format.

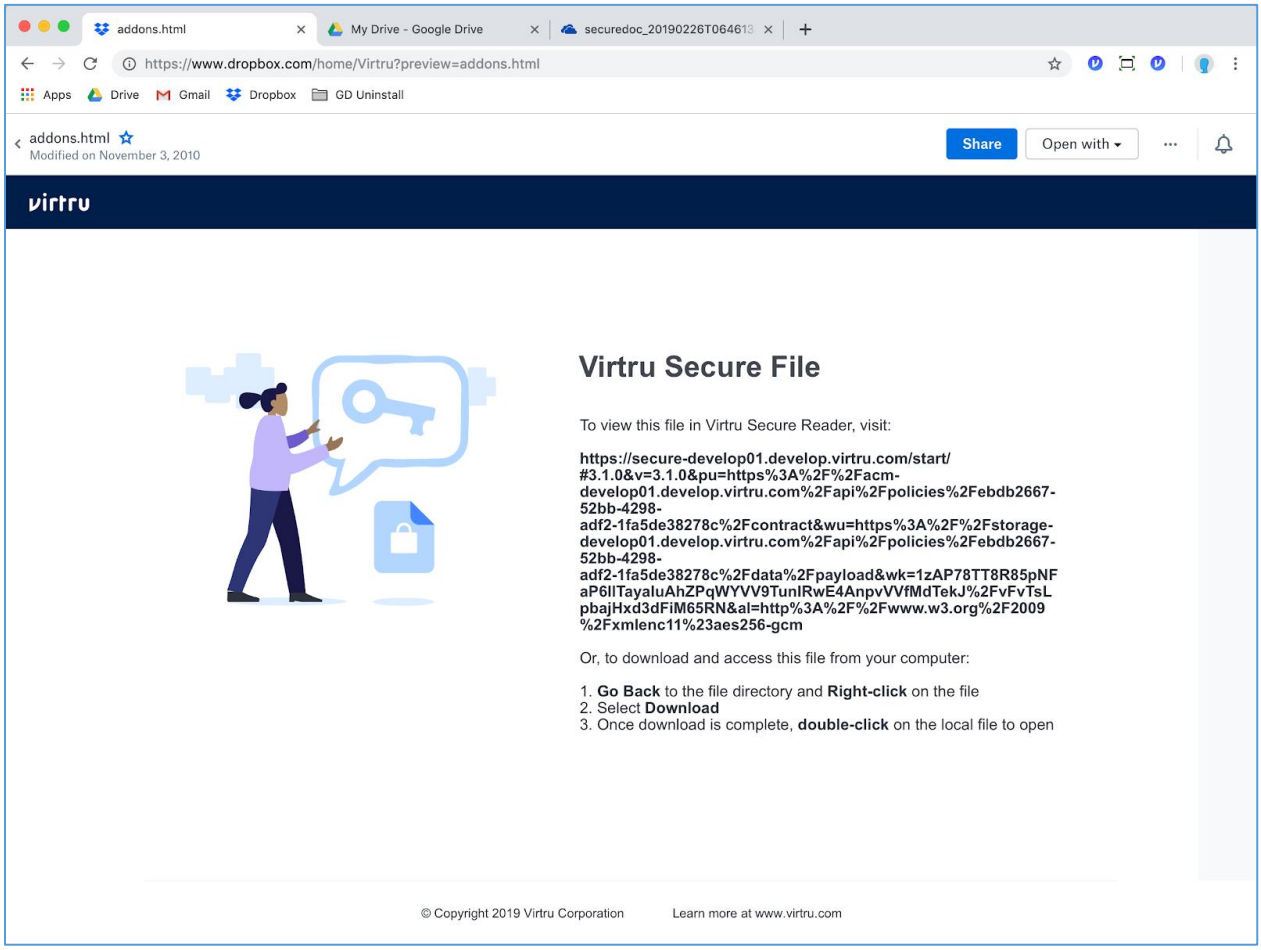


Any time this user or another party tries to open the downloaded .tdf.html file, they will be forced to authenticate in their web browser prior to seeing the secure file in Virtru's Secure Reader. Unauthorized users will not be granted access. This is how Virtru is able to persistently protect the file regardless of where the file is stored.



While files protected with PFP are only viewable in Secure Reader, Virtru provides guidance to users attempting to access protected files in third party cloud services like OneDrive,

Google Drive, and Dropbox. Users are notified that the file they are attempting to access is a Virtru Secure File and are directed to Secure Reader to view.



Request Access Workflow

Although Virtru PFP restricts access to only authorized users, new (unauthorized) users are allowed to request access to a file. If someone requests access to a file you own, you will receive an email notification from Virtru. Access is then managed through the Virtru Dashboard.

Re-Shared Attachments

To ensure a file remains protected no matter where it goes or who shares it, Virtru has introduced the concept of Re-Shared Attachments with Persistent File Protection. A file with Persistent File Protection becomes a re-shared attachment when someone other than the original owner shares the file. Any user who is not the original file owner is unable to change the privacy settings on the file that is being shared.