



Sending Digital Information Safely

As a UVic employee, you receive and distribute a variety of digital information. Once you have determined the security classification of information you are handling, you need to consider the safest way to send the information.

Before sending information through email, consider the contents of your message. Ask yourself if there is sensitive information contained within the:

- text of your message
- messages you are forwarding
- attachments on the email thread

Common errors and solutions when emailing

 Error	 Solution
Sending an email to the wrong recipient	<ul style="list-style-type: none"> • Disable auto-complete. See instructions at Turning Off Auto-complete • Select the recipient from your address book or Global Address List • Encrypt attachments to prevent unauthorized users from opening • Information about encrypting files can be found at the University Systems Help Centre website in the “Common applications supporting file encryption” section, or directly at the following links for encrypting these file types: <ul style="list-style-type: none"> ▪ Microsoft Word ▪ Microsoft Excel ▪ Adobe Acrobat ▪ 7-Zip
Replying to a mailing list or Replying All when you meant to send the message to a specific recipient	<ul style="list-style-type: none"> • Carefully review the <i>To:</i> field of all outgoing messages • Depending on who you are forwarding the message to, consider removing sensitive information
Prematurely sending a message before removing sensitive information	<ul style="list-style-type: none"> • Review all attachments prior to populating the <i>To:</i> field • Add potential recipients after you are satisfied with your message
Sending the wrong attachment in an email	<ul style="list-style-type: none"> • Consider alternative methods for transmitting information (see below) • Encrypt file to prevent unauthorized users from opening



There are more secure options than e-mail

While e-mail can be a convenient way to exchange information, there are methods that significantly reduce the threat to information security.



[OneDrive](#)



[Connect](#)

(SharePoint)



[Shared Drive](#)

(Departmental File Share)

Alternative methods for transmitting information for Internal, Confidential, and Highly Confidential Information

Provide the recipient with instructions to access information in the system of record

Example: providing the name of a pinned report in FAST

Why? This avoids the risk of exporting this information to an unencrypted file that may be insecurely transmitted or stored.

Other benefits: Creating a report in the system of record allows your recipient to securely access the latest version of the data rather than a point-in-time snapshot of the data that may change over time.

Send a link to a document stored on Connect or a Departmental File Share

Example: sharing a class list containing student personally identifiable information with TAs, co-instructors, or other staff

Why? If the document is not attached, it eliminates the risk of sending the document to the wrong recipient as anyone with the link would need to sign in with their NetLink ID to access your document. Depending on whether you are sharing or collaborating, you may need to lock the document against editing.

Other benefits: Collaborating on a single copy of the document ensures you are not left to merge different or conflicting changes to arrive at a final version. Everyone can view all comments and edits.

Share a document using OneDrive

Example: providing information regarding academic concessions for students

Why? OneDrive provides a link to a single copy of the document and any recipient will need to sign in with their NetLink ID to access the document. Information on how to share OneDrive Files and Folders can be found at [Share OneDrives Files and Folders](#).

Other benefits: In addition to collaboratively editing a single copy of the document, you can specify the length of time that access should be provided to your collaborators before it is automatically removed. Great for short-term projects or consultation!

If you require further assistance, please contact the [Information Security Office](#).



The Sending Digital Information Safely Tip Sheet is licenced under a [CC-BY-NC-SA 4.0 International Licence](#).
June 2021 | Developed by the University of Victoria.