

Email Attachments: Best Practices

Students, staff and faculty now communicate very well by email. There are simple things you can do to use email even more effectively to get your message across¹.

1 Sending Email Attachments

1. Send the message in the body, not in an attachment.

Avoid using attachments if you can send the message in the body instead. Some email reading tools do not handle attachments well. Using attachments makes the recipient take extra steps to read your message. Attachments are the primary way viruses are transmitted. Attachments are often in a proprietary format (such as Word, Word Perfect, Excel, and so on) that the recipient might not have the software to read. That software can be expensive, and might not work on every operating system. Reading attachments in proprietary formats is especially hard for recipients who use Unix or GNU/Linux or who lack the funds to upgrade proprietary software annually.

2. Use non-proprietary formats.

If you want more formatting than a simple email message can provide, consider using a non-proprietary format such as HTML (.htm, .html), Rich Text Format (.rtf), or Portable Document Format (.pdf) in preference to proprietary formats such as Word (.doc). More people will be able to read your message; there is a smaller chance you will inadvertently transmit a virus; there is a smaller chance you will compromise your own privacy accidentally; and you will save University resources—the files are much smaller. You can use your usual word processor to write documents but still save them in a more accessible, compact and safer format to send them by email. [Help is available](#) to learn how to save documents in these formats. The pros and cons of several common document formats are [tabulated below](#). Security risks, privacy compromises, and hidden costs inherent in email attachments are detailed in the [appendix](#).

3. Attachments are a way to send files, not messages.

However, if you really need to send a file (such as a spreadsheet) to a particular individual so that person can work with it, attaching the file to an email message can be an effective way to transmit it—if the file is not too large. If you just want the recipient to be able to read or print the information, send the information in the body of the message or use a non-proprietary format: there is a better chance the recipient will be able to read your message.

Email attachments should be used to send only moderately-sized files (less than 0.5MB or so) to a small number of recipients (up to 10 people). Larger files or larger recipient lists can cripple email servers. If a large number of people need to work with a large file, consider posting the file to a web site and sending just the URL by email, or transferring the file using [FTP](#) or [SFTP](#).

Thank you for taking the time to read this.

Remember: Think Before you Click!

¹©2003 University of California at Berkeley—Educational Technology Committee. Previous drafts of this document are available here: [2nd draft](#), [1st draft](#). This document is located here: [PDF](#).

2 Email Attachment File Types: Pros and Cons

Format	Editable?	Cross Platform?	Secure?	Compact	Proprietary	Advanced Formatting?	Permanent	Cost
Plain Text ASCII (TXT)	Yes	Yes	Yes	Yes	No	No	Yes	Free
HyperText Mark-up Language (HTML,HTM)	Yes	Yes	Variably [1]	Yes	No	Yes	No	Free
Portable Document Format (PDF)	No	Yes	Mostly [2]	Yes	Yes	Yes	Largely [3]	Free
Rich Text Format (RTF)	Yes	Partly	Yes	Yes	Yes	Some [4]	Yes	>\$5
Word Document (DOC)	Yes	No	No	No	Yes	Yes	No	>\$20

Notes:

- [1] Often HTML that is authored within an email program (such as Eudora or MS Outlook) is secure. However, HTML email that you receive can have web bugs or other security vulnerabilities. It is important to understand what the default security settings of your email program are and that the default settings can be insecure. Some things you might want to do are 1) turn off cookies within emails, 2) not allow scripts to run in emails and 3) open your email off-line to avoid web bug tracking.
- [2] PDF is largely a secure format. It does allow some basic scripting and URL linking which can be used to run programs on your system and to track where the document is being viewed on the Internet.
- [3] PDF undergoes changes regularly although it is expected to remain backward-compatible.
- [4] Some advanced formatting is available in RTF.

3 APPENDIX: Details of Security Risks, Privacy Compromises, and Hidden Costs

Attaching documents to email is often unnecessary, costly, exclusionary and risky, and transforms UC Berkeley in a way that burdens some units financially. This can be illustrated by looking at one of the most common email attachment formats: Microsoft Word. (For example, minutes and agenda of administrative and Academic Senate committee meetings are often sent as Word email attachments.) Some of the following discussion is specific to Word Documents but most of the comments apply to email attachments in general.

3.1 Cost

- A Word document is typically 5-10 times larger than the equivalent information in a plain-text (ASCII or .txt) file. Using Word instead of plain text requires 5-10 times more computer disk space, bandwidth usage and transmission time—which can be significant for users with low bandwidth connections. Email messages with multiple recipients are copied and stored as many times as there are recipients. This increases the rate at which storage resources are exhausted.
- Using Word documents increases dependence on proprietary software and limits the competitive ability of other software products². UC Berkeley is becoming a *de facto* Microsoft campus. Because Microsoft standards are proprietary and change rapidly, this requires significant campus outlays to keep software up-to-date, even if newer versions offer no meaningful functional improvement. Freeware, shareware, and other vendors' software is only partially able to use files written for Microsoft applications, because Microsoft does not publish its complete file specifications. Reliance on proprietary file formats when open standards provide the same function exposes the University to unnecessary long-term financial and operational risk.

3.2 Exclusionary Impact

- Word documents pose access problems. Unix users, GNU/Linux users, people who use public terminals (without file creation privileges), people who use web email interfaces, and people who use Palm OS devices to read email often cannot read Word documents. Even Windows and Macintosh users must take extra steps to read Word attachments (scan for viruses, save to disk, read with the word processing application).
- Word documents posted to UC Berkeley websites are not accessible to the widest global audience—only to those with the means (and platform) required to use a current version of Word. This bias excludes poorer members of our international audience. Because the Word file format changes every few years, a document written today may not be readable using future versions of Word. Moreover, those with older versions of Word are not able to read documents written in newer versions.

²By limiting the utility of other software products—such as the free operating system BSD, developed here at UC Berkeley—we are limiting our options and increasing costs. see: <http://www.gnu.org/philosophy/no-word-attachments.html>

3.3 Security and Privacy

- Word documents can compromise the author's privacy and the recipient's privacy and security. Word documents often contain previous drafts, corrections, marginal notes, pieces of unrelated documents, and information about the computer system that was used to create or edit the document.
- Word attachments can expose the recipient to viruses, worms, and "web bugs" that track where on the Internet the document is being read^{3,4}.

Word has features to track changes in documents by several co-authors. When a group of authors collaborates on a document they have agreed to write in Word, it can be appropriate to send the manuscript back and forth by e-mail. However, Word documents are used principally for the formatting capabilities of Word, not for more advanced features. Unless the advanced features are really needed, there are advantageous alternatives to Word, depending on the amount of formatting the user desires: plain text (TXT), hypertext (HTML), Adobe's Portable Document Format (PDF) and rich text (RTF). The features and limitations of these formats are delineated in the [table in the body of this document](#).

The alternative formats are much safer for the sender and the recipient. (However, note that when a Word document is saved as html, which preserves much of the formatting and makes the document more accessible, Word embeds potentially sensitive information in the html document.)

In conclusion, please be sensitive to accessibility, security, and cost when you send email. Send plain text in the body of the message when that will get your message across. If you need more advanced formatting to achieve your goals, use the safest and most accessible format you can. Send (or post) final versions of formatted documents in HTML or PDF.

References

[Help is available... Saving in different formats:]

- Windows Users:
 - [Saving Word 97/98/2000 as text or HTML](#)
 - [Saving Word as RTF](#)
 - [Printing to PDF \(involves printing to Postscript and then converting to PDF\)](#)
 - Other Possible Resources: [ePrint](#) from LEADTOOLS, [Free PDF](#) (free, requires RedMon and GhostScript), [Jaws PDF Creator](#), [PDF Converter](#), [PDF Driver](#), [pdf995](#), [pdfFactory](#), [pdfMachine](#), [Win2PDF](#) (Windows 2000 or NT, adds a nag page to the document until purchased).
- Macintosh Users:
 - OS X: "In Mac OS X it is easy for users to save a document as a PDF. All the user needs to do is open the Print dialog and click the Save As PDF button.

³See Symantec's Gallery of the Word Macro Virus Family:
<http://www.symantec.com/avcenter/venc/data/acro.html>

⁴See The Privacy Foundation's FAQ on Document Web Bugs:
<http://www.privacyfoundation.org/resources/docbug.asp>

The user then provides a name for the PDF and chooses a location for the file.”
Quoted from [apple.com](#).

- OS 9 (and earlier): You will need to download the [”Print to PDF”](#) extension or upgrade to OS X.
- GNU/Linux and Unix users:
 - Print to a postscript and then convert using ‘ps2pdf’ (which is more than likely [already installed on your system](#)).

[(S)FTP:] FTP stands for ”File Transfer Protocol.” FTP is the standard way to transfer files over the Internet. SFTP is a secure version of FTP that encrypts all information, including passwords. Mac OS X and most Linux distributions include both ftp and sftp (type ‘which ftp’ or ‘which sftp’ at a terminal command-line prompt to see if your system has it installed.) Most Windows systems and older versions of Mac OS include FTP but not SFTP. The programs SSH and MacSSH—available from [software.berkeley.edu](#)—provide SFTP for Windows and Mac OS, respectively.

About this document: This document was written in [L^AT_EX](#) and translated to PDF using [dvipdfm](#) and the [hyperref](#) package. The HTML was created using [L^AT_EX2HTML](#)⁵. Last modified 4 May 2003 by [Joseph Lorenzo Hall](#) (jjhall@astron.berkeley.edu).

⁵The following command was issued to [L^AT_EX2HTML](#):
`latex2html -split 0 -nonavigation -noinfo -noaddress attachments.tex`