# Communicating FERPA-protected

# Student Performance Information with the Internet

*Never send (communicate) information about student performance using electronic mail!*

Using electronic mail to communicate student performance information—like information about your personal health—does nothing to protect that information from capture and use by anyone on the Internet. Would you like anyone to view and gossip about your performance or your health?

Electronic mail uses a local application to send and receive packages of information across the Internet to and from a computer with a “mail service” someplace on the Internet. The computer with the mail service is called the “mail server”, and it handles messages in many ways for the people that use the mail service. You recognize mail services by names such as “Webmail”, “gMail”, “Hotmail”, “YahooMail”, and so on.

Simply put, you, through your mail application, send a message to a mail server, and the mail server delivers the message to your intended recipient through his or her mail application. Each mail service that you use gives you an “electronic mail address” so that anyone can find you and send you messages.

Your messages are sent into and out of the mail service as packages of information, and the packages have a particular, well-known format that allows everyone’s local mail application and everyone’s mail service to read, write, and understand all those messages. That format is called the “Simple Mail Transfer Protocol (SMTP)”, and it is so simple, convenient, and cheap that almost everyone has one of more electronic mail addresses.

Nevertheless, you get what you pay for (and you don’t get what you don’t pay for): *You do not get privacy.* You know that through SPAM, but you should also know that not only are electronic mail addresses public, but so is the content of your messages! You might not know this unless you sent your SSN through electronic mail and someone “stole your (financial) identity,” but everyone should keep this in mind.

If my computer is on the same part of the Internet that you use to send your electronic mail messages, I can grab those messages--just in case they were being sent to me ;-). I could also read those messages because the whole of the message is easily readable (clear) text. Here is an actual message:

|  |
| --- |
| MIME-Version: 1.0In-Reply-To: <rt-4.0.7-19705-1389287263-848.812371-0-0@cc.uic.edu>X-Mailer: MIME-tools 5.427 (Entity 5.427)Content-Disposition: inlineReferences: <RT-Ticket-812371@cc.uic.edu> <CAHt4ky-Nz\_4uNtya3KbyfDX4YyCDPUwDE+nYUyzTJawJMUoTiA@mail.gmail.com> <rt-4.0.7-23902-1388855353-126.812371-5-0@cc.uic.edu> <009601cf0b07$3959d960$ac0d8c20$@edu> <rt-4.0.7-31094-1389030369-1072.812371-19-0@cc.uic.edu>, <rt-4.0.7-31417-1389278961-1419.812371-19-0@cc.uic.edu> <56A6DFD833CF7D48A0F1989A561EBDE49C2DE6@CC-X10MBX1.ad.uic.edu> <003801cf0d5d$637734b0$2a659e10$@edu> <rt-4.0.7-19705-1389287263-848.812371-0-0@cc.uic.edu>Content-Type: text/plain; charset="utf-8"Message-ID: <rt-4.0.7-26584-1389288327-1833.812371-0-0@cc.uic.edu>Content-Transfer-Encoding: binaryX-RT-Original-Encoding: utf-8RT-Send-CC:X-RT-Encrypt: 0X-RT-Sign: 0Content-Length: 7630\*\*\*\*\*\*\*\*,I noticed just now that your \*\*\* Orientation link goes to an MP4 file in the Content System. (I was looking at the Recording in Bb Collaborate, which was not working until just now.) The file in the Content System does not permit access to \*\*\*\* \*\*\*. Giving \*\*\*\* \*\*\* Read Access Permission ought to do the trick.What about the calendar?Michael. |

Unless you and your recipient go through the trouble to set up (say, PGP) encryption, get your recipient’s encryption key, and encrypt the message body before you send it, the contents of your message is as easily readable as the one above. That’s a lot of trouble, so most people do not go through the trouble unless the message is really important to them and the only way to send it is through electronic mail.

The lack of encryption, that is, purposeful and reversible scrambling, for electronic mail messages is the reason you so often hear that you should not send SSNs, passwords, or other personal information through electronic mail.

Would you mind if someone else sent out information about your health, your performance as an employee, or your performance as a student using electronic mail? Of course, you would not—especially knowing now that anyone could read and use that information (perhaps against you)!

This is such a problem for individuals that the Federal Government has made it a crime to disclose such information and has allowed victims to sue for damages in civil courts.

Think of it. But what if a student brought the Federal Government and the civil courts after you and the University for wanton exposure of their performance in course(s) at the University to anyone and to everyone on the Internet? Do you think that the University will think kindly of you if this happened?

There are ways to protect yourself:

 *Never send (communicate) information about student performance using electronic mail!*

Yes, you need to communicate. So, you have to communicate about student performance in a secure manner. You need a local application (and a service) that knows how to encrypt and decrypt messages and other information transferred across the Internet and that automatically does so.

The University has at least three: Outlook-Exchange, Box, and Blackboard Learn. All three of these services use the web browser of your choice. When you use one of these services, notice that the URL with which your browser is communicating (up in the “location” box) starts with [https://](NULL) and that there is often the symbol of a closed padlock nearby. Web browsers know how to encrypt and decrypt your messages send across the Internet, and that URL and icon indicate that browsers are protecting your information.

Using the Outlook (or Entourage application on your “Desktop” or the Outlook Web App in your browser with the UIC Exchange mail (and calendar) service *protects your electronic mail* unlike Webmail, or gMail, or whatever else you might think of off the top of your head. Using the <http://uofi.box.com> “cloud” file service to exchange and share files protects your files when they are saved on and transferred across the Internet. (Saving your attachments on uofi.box.com can also save you time by allowing you to show the original file to a late comer to your conversation and to show everyone the most recently edited version without a thought.) Using the “Messages” feature within Blackboard Learn—not the “Send Email” feature—or the “Journal” feature within Blackboard Learn allows you as the instructor to have a private (encrypted) channel to discuss performance (bad and good) with any and each student individually.

So, *think before you send*, and get comfortable using these tools to protect performance information about your students and to protect yourself and the University from the cost of criminal charges and civil damages.

Michael G. Prais, Ph.D.

ACCC Instructional Technology lab