E-Mail Basics

Robert F. Loftus, MSLIS

Creating Strong Passwords

A strong e-mail password is Alpha-Numeric, contains upper and lower-case letters, and is not "password" or the name of your hometown. The longer your password is, the better. The greater the number of numbers or letters in your password, the harder it becomes for someone to guess it.

Bad Password: "password" or "1234"
Good Password: "HAHA*password*1234"
Bad Password: "bville"
Good Password: "Baldwinsville13027NY"

Also remember that when you go back to your e-mail account and enter your password there's no such thing as "almost right", it's like a combination lock – all or nothing.

New or Compose

The first step to sending a new e-mail is clicking on the new message button. This button is usually marked by the word "New" or "Compose". Clicking on the new message button will open a text editor window where you may begin typing your message. Below are several examples of what a typical "Compose" or "New Message" button may look like.
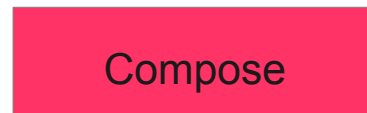
The E-mail Address and Text Editor Windows

To: This is who you're sending the e-mail to. You put the person's e-mail address into this field.
CC: This stands for "Carbon Copy", and it allows you to enter a second recipient's e-mail address.
Subject: This is where you tell the person what the e-mail is about. Be as specific as possible. One word subject lines often result in e-mails being snagged by the spam filter.
Text Editor Window: This is the part of the e-mail where you type your actual message. The Text Editor usually has a *Control Bar* at the top, which allows you to adjust your font, or insert images into your message.

An example of what a typical e-mail Text Editor control Bar looks like.

Sending Attachments

Attachments are files that are sent along with your e-mail. Add an attachment to an e-mail by clicking on the attachment button while you have your text editor window open. The attachment button may be marked by a paper clip icon, a push-pin icon, or the word "Attachments".

Receiving Attachments
Attachments in e-mails you receive are marked by a file icon. Double-clicking on the icon will usually download the attachment to either your Documents or Downloads folder. When you double-click on the filename after downloading the file, your computer should open that file in whatever program is the default for that file type – so if you download an MP3 file, that file should open in your media player. If you download a .doc file, the program should open in Microsoft Word or OpenOffice Writer. If you download a pdf file, the file should open in Adobe or Foxit Reader.

Reply and Forward
Reply will allow you to respond to an e-mail that's been sent to you. It is not necessary to recreate the business letter format of an original e-mail with a Reply. Forward allows you to forward an e-mail on to a different recipient. Once again it is not necessary to create a new formatted letter, a brief one or two sentences explaining why you forwarded the document is sufficient.

Deleting e-Mail
To delete an e-mail while you are looking at it just hit the "Delete" button in your e-mail toolbar. To delete multiple e-mails check the boxes in front of each e-mail in your Inbox and hit the Delete button in your e-mail toolbar. It's important to delete junk e-mails and only save the important ones.

The Spam Button
When you have an e-mail open, clicking on the "spam" button moves that e-mail to your spam folder. It will also black-list that e-mail sender so that any future e-mails from that sender are automatically routed to your spam folder, rather than your Inbox. If something goes into spam and you want it in your Inbox, you have to find that e-mail in your spam folder, Right-Click on the subject line of the e-mail and select "Move to > Inbox". This also white-lists the sender, so their mail won't be automatically routed to your spam folder in the future.

Avoiding Viruses
File extensions refer to the three to four letter codes at the end of a file name. The two file extensions that are most commonly associated with computer viruses are ".exe" and ".dll". Never open an attachment with one of these extensions unless you know exactly who sent the e-mail, and why.

Don't download attachments unless you know who sent the attachment.

If your e-mail provider has a built in anti-virus scanner that tells you a file is infected, then don't open that file.

Phishing Scams
Phishing scams are methods that identity thieves use to steal financial information. These often involve e-mails that are made to look like messages or offers from banks. Learn the web address for your bank and never respond to an e-mail that claims to be from your bank but which comes from another web address.

For example, if you use M&T bank then all e-mails should come from a server with "@mtb.com" at the end of the e-mail address. Likewise, any forms that are linked to in an e-mail from M&T bank must be at a web address that begins with "https://www.mtb.com/..." Never enter information into a form which claims to be from M&T bank but which has a different web address.

IF you aren't sure, then call the bank before you fill out any on-line forms. If you are working with a good bank they'll be able to tell you if any e-mail campaigns are underway and will be able to describe the e-mail that was sent to you. If you call your bank but the customer service staff claim they have no knowledge of any on-line promotions and cannot tell you whether the e-mail is legitimate or not, then it means that either the e-mail you received is a fake, or the bank is poorly managed and it's time to think about taking your business elsewhere.